BEC 6800RUL

4G/LTE Outdoor Router

User Manual

Version release: v1.3

Last revised: Sept, 2015

TABLE OF CONTENTS

TABLE OF CONTENTS 2

CHAPTER 1: INTRODUCTION 1

INTRODUCTION TO YOUR ROUTER 1

FEATURES & SPECIFICATIONS 2

HARDWARE SPECIFICATIONS 3

APPLICATION DIAGRAM 3

CHAPTER 2: PRODUCT OVERVIEW 4

IMPORTANT NOTE FOR USING THIS ROUTER 4

PACKAGE CONTENTS 4

DEVICE DESCRIPTION 5

MOUNTING INSTRUCTIONS 6

CHAPTER 3: BASIC INSTALLATION 13

NETWORK CONFIGURATION – IPV4 14

Configuring PC in Windows 7 (IPv4) 14
Configuring PC in Windows Vista (IPv4) 16
Configuring PC in Windows XP (IPv4) 18
Configuring PC in Windows 2000 (IPv4) 19
Configuring PC in Windows 98/ME 20
Configuring PC in Windows NT4.0 21

NETWORK CONFIGURATION – IPV6 22

Configuring PC in Windows 7 (IPv6) 22
Configuring PC in Windows Vista (IPv6) 24
Configuring PC in Windows XP (IPv6) 26

DEFAULT SETTINGS 27

CHAPTER 4: BASIC CONFIGURATION 28

LOGIN TO YOUR DEVICE 28

STATUS 29
QUICK START 30
WAN 32
CHAPTER 5: ADVANCED CONFIGURATION.....33
LOGIN TO YOUR DEVICE 33
STATUS 35
Mobile Status 36
ARP Table 37
DHCP Table 37
System Log 38
Firewall Log 38
UPnP Portmap 39
QUICK START 40
CONFIGURATION 42
LAN - Local Area Network 42
Ethernet 42
IP Alias 42
DHCP Server 43
WAN - Wide Area Network 45
WAN Profile 45
System 50
Time Zone 50
Firmware Upgrade 51
Backup / Restore 53
Restart Router 53
User Management 54
Mail Alert 55
Firewall and Access Control 56
Packet Filter 57
MAC Filter 59
Intrusion Detection 60
Block WAN PING 62
URL Filter 62
QoS - Quality of Service 65
Quality of Service Introduction 65
QoS Setup 65
Virtual Server 70

Port Mapping *71*
DMZ *73*
Time Schedule 75

ADVANCED 76
Static Route *76*
Static ARP *76*
Dynamic DNS *77*
Device Management *78*
SIP_ALG *85*
IGMP *85*
SNMP Access Control *86*
TR-069 Client *88*
Remote Access *89*

SAVE CONFIGURATION TO FLASH 90

RESTART 91

LOGOUT 92

CHAPTER 6: TROUBLESHOOTING 93

Problems with the Router 93
Problem with LAN Interface 93
Recovery Procedures 94

APPENDIX: PRODUCT SUPPORT & CONTACT 95

CHAPTER 1: INTRODUCTION

Introduction to your Router

Thank you for purchasing **BEC 6800RUL 4G_LTE Outdoor Router**. This unit is a light-weight, an industrial-grade outdoor fixed wireless router with an IP67 rated enclosure to withstand extreme weather conditions and harsh rugged deployments. With integrated IEEE802.3af power over Ethernet (PoE) support, the 6800RUL provides an easy installation from eliminating the need for a separate power and data cable.
In addition to outdoor, it can be installed in environments such as: manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses or virtually any venue requiring a robust wireless solution. The 6800RUL integrates a high performance device with an embedded LTE module and advanced IP networking features enabling support of multiple high bandwidth applications at peaks speeds up to 100Mbps downlink and 50Mbps uplink.

Lightweight, Compact and unobtrusive Design

With multiple mounting options and a light weighted, it is easily to install the 6800RUL by single person. The 6800RUL also has a built-in passive Power of Ethernet (PoE) so both data and power can be sent from the unit.

Designed for Challenging / Rugged Deployments

The 6800RUL is designed for the toughest industrial environments. With IP67 hardened enclosure with Industrial-grade components, the 6800RUL can be installed in manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses, etc.

4G/LTE Mobility

With 4G/LTE-based Internet connection (4G/LTE embedded module, requires an additional SIM card), you can access to the Internet through 4G/LTE whether you are seated at your desk or taking a cross-country trip.

4G/LTE Management Center

With the **BEC 6800RUL (4G_LTE Outdoor Router)**, monitoring your 4G connection status is a breeze, unique 4G Management Center is an utility tool displaying its current 4G-signal status visually for users to maximize their connection. You can monitor the bandwidth with the current upload and download speed. This too also calculates the total amount of hours or data traffic used per month, allowing you to manage your 4G monthly subscriptions.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Features & Specifications

- 4G embedded with a built-in SIM card slot
- High-speed 4G connection up to downlink 100Mbps and uplink 50Mbps data rate
- 4G Management Center for connection monitoring
- Firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ideal for homes, businesses, rural areas and the underserved

LTE Antenna Options

- Embedded MIMO Directional (700MHz): 6~8dBi

OR

- Two (2) detachable MIMO N-type: (N Models)
  - ✓ OX-7 Antenna (700MHz): 5dBi
  - ✓ OX-17 Antenna (1700~2100MHz): 9dBi

Network Protocols and Features

- NAT, static routing and RIP-1 / 2
- NAT supports PAT and multimedia applications
- Transparent bridging
- Virtual server and DMZ
- SNTP, DNS relay and DDNS
- IGMP snooping and IGMP proxy

Firewall Management

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Remote access control for web base access
- IP, MAC, and URL filtering
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization based-on IP protocol, port number and address

Management

- 4G Management Center
- Web-based for remote and local management
- Firmware upgrades and configuration data upload / download via web-based interface
- System Log monitoring
- Supports DHCP server / client / relay

Hardware Specifications

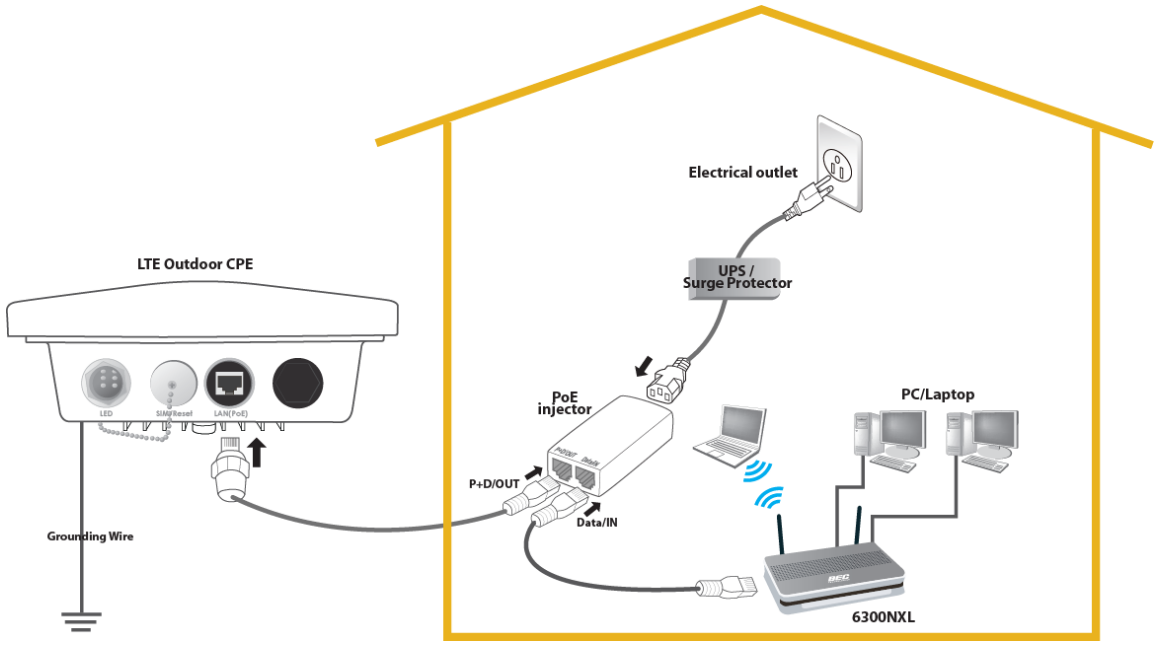
Physical interface

- 10/100 Ethernet LAN with IEEE802.3af compliant PoE PD
- SIM slot: (for the SIM card from Telco / ISP)
- LED Indicators: Power, LAN (PoE), Boot, LTE, and Internet

Physical Specifications

- Dimensions (W*H*D): 8.5" x 7.5" x 3"(257mm x 227mm x 91mm)
- Weight: 2.75kgs (6.06lbs)
- IP-67 Grade Enclosure

Application Diagram



CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

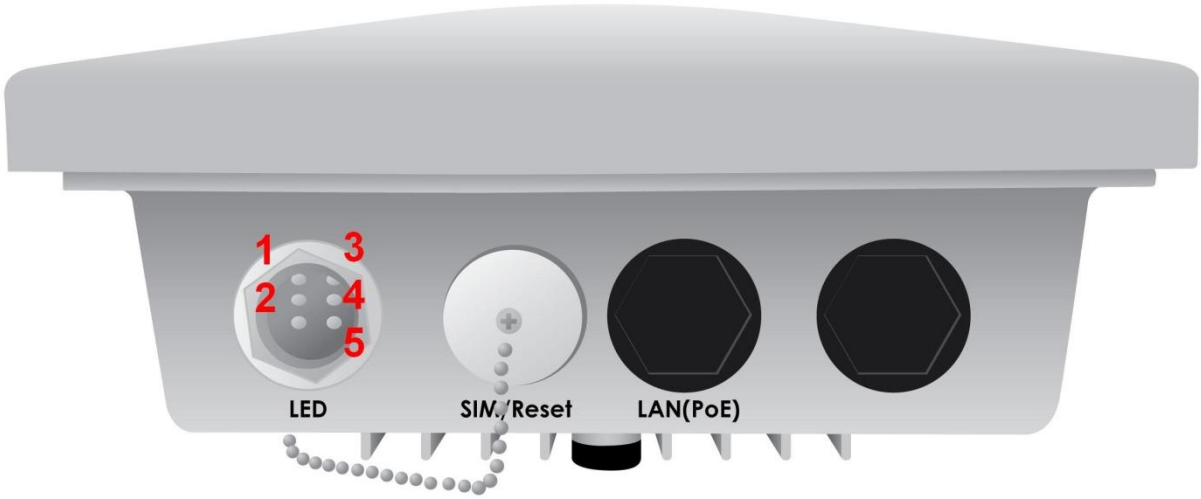
Attention

- ✓ Do not remove, open or repair the case yourself. Contact with your Internet Service Provider or have it repaired at a qualified service center.
- ✓ Use the supplied PoE (Power-over-Ethernet) injector for indoor only or with any 802.3at capable PoE injectors to connect with BEC 6800RUL
- ✓ It is mandatory to earth ground the BEC 6800RUL. Improper grounding not only could damage the unit but also all eqiupments connected to it.

Package Contents

- ✓ **BEC 6800RUL 4G/LTE Outdoor Router**
- ✓ **This Quick Installation Guide**
- ✓ **M25 Cable Gland**
- ✓ **25ft Outdoor LAN cable**
- ✓ **PoE Injector**
- ✓ **Grounding Wire**
- ✓ **Mounting Kit**

Device Description



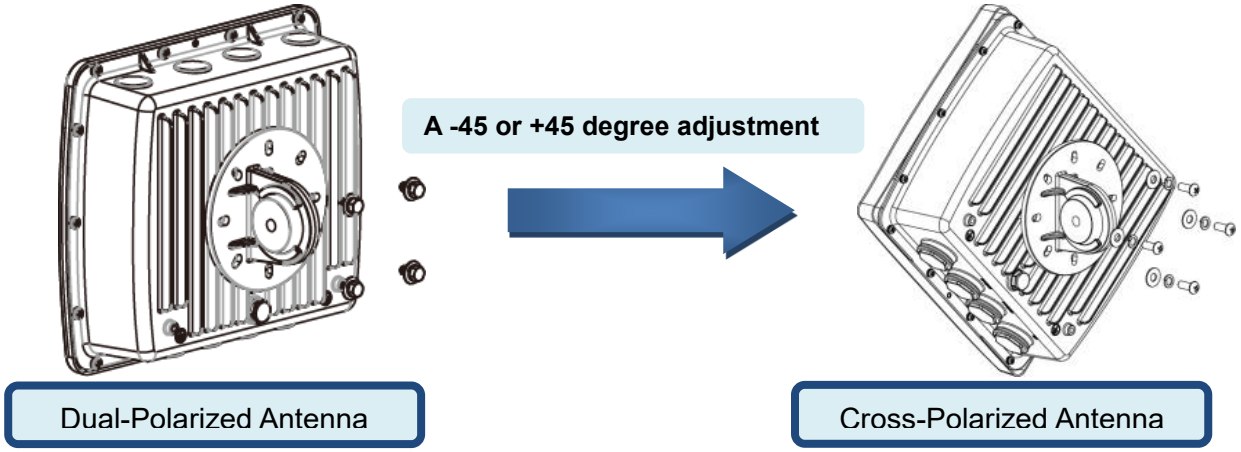
CONNECTORS	DESCRIPTION
SIM/ Reset	Insert the SIM card into the SIM slot; press the reset button to reset device or restore to factory default settings
LAN(PoE)	Connect to a computer/ Passive PoE using an Ethernet cable.

LED		DESCRIPTION
LED	**1. Power**	Lit green when system power on.
	2. LAN(PoE)	Lit green when the LAN port is connected to an Ethernet device. Blink when data is being transmitted/ received
	3. Boot LED	Lit green means system boot up successfully.
	4. LTE	Lit green when 4G/LTE service is ready to precede the dial-up.
	5. Internet	Lit green when Internet is available.

Mounting Instructions

1. Attach the Articulation Pole to the Enclosure

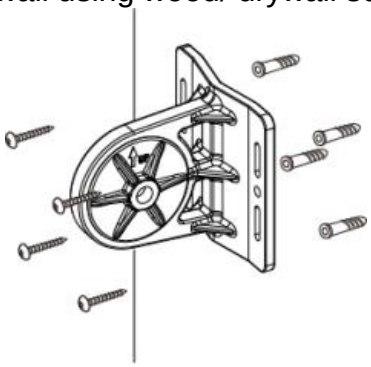
Attach the articulation pole to the back of the BEC 6800RUL using M6*16 screws and washers.



2. Mounting on Wall or a Pole

2.1 Mounting on Wall

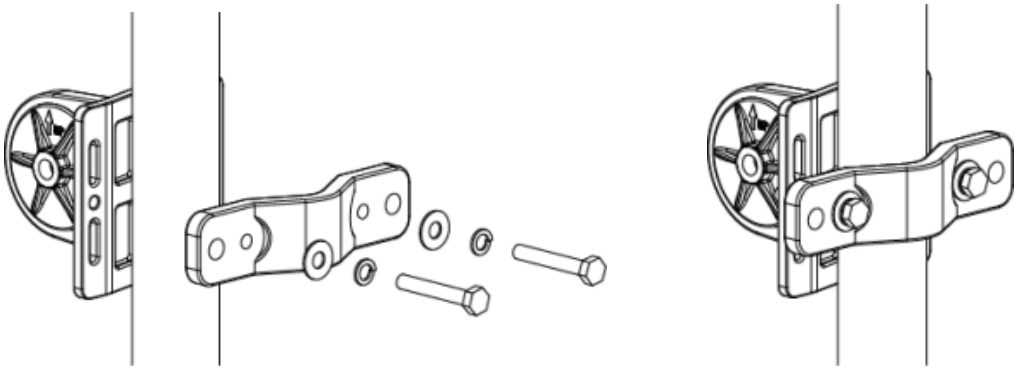
Fix the T-formed Bracket to the wall using wood/ drywall screws.



2.2 Mounting on a Pole

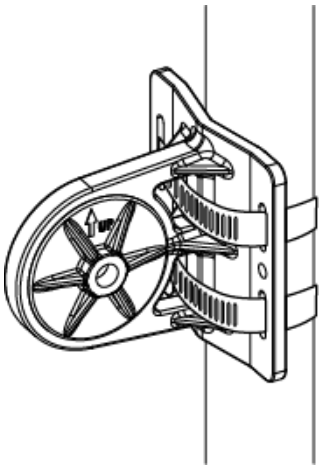
2.2.1a Mounting for pole <u>smaller</u> than 1.5” (38mm)

Attach the T-formed Bracket and the W-bar to the pole then use M6x60 bolts, spring washer and washer to fix the mounting kit onto the pole.



2.2.1b Mounting for pole larger than 1.5” (38mm)

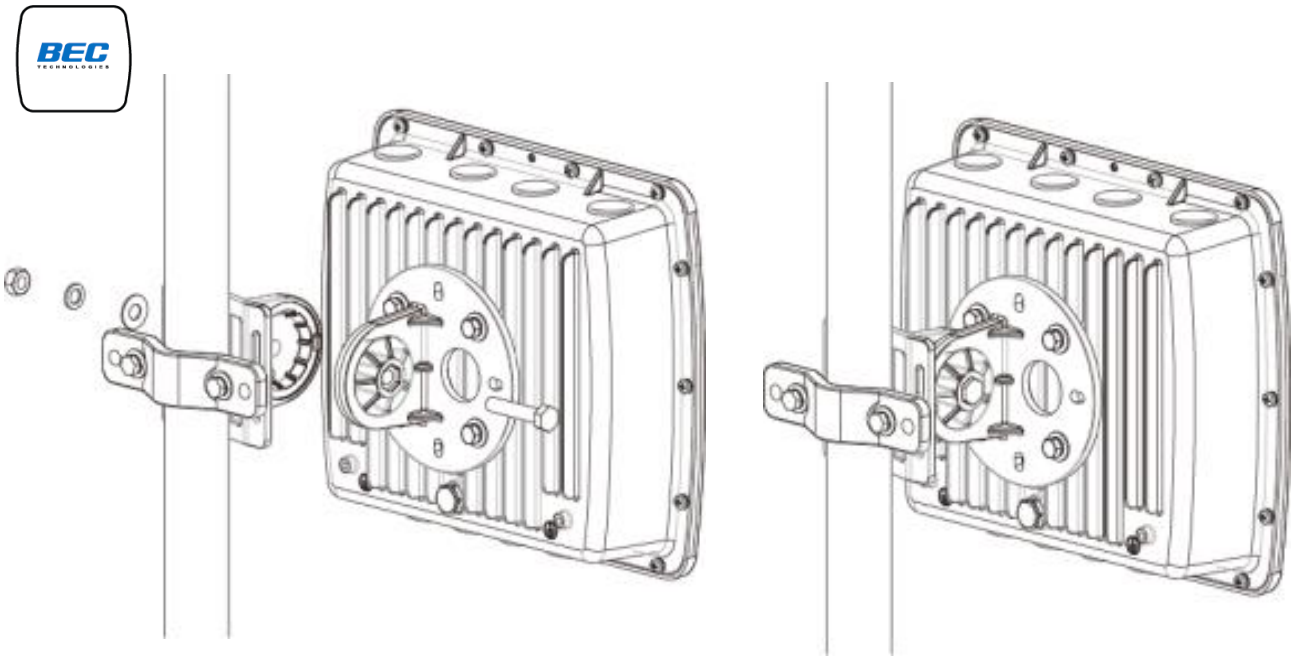
Fix the T-formed Bracket to the pole by using the stainless hose clamp.



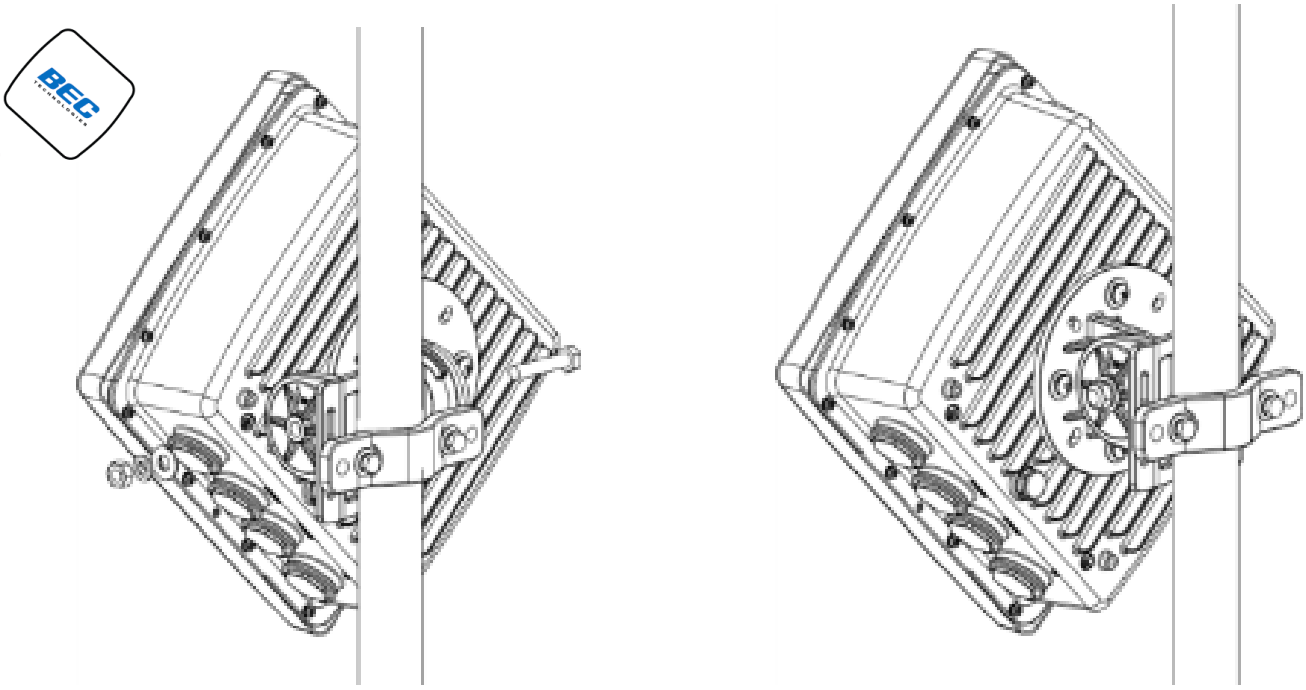
2.2.1 Mounting BEC 6800RUL on a Pole with T-formed Bracket

Attach the articulation pole to the T-formed bracket by using M8x40 bolts, nut, spring washer and washer.

Dual-Polarized Antenna – The original of the source position, the nominal position, is seeing **BEC logo** when facing toward the 6800RUL,



Cross-Polarized Antenna – From the nominal position, adjusting and rotating the 6800RUL -45 or +45, anticlockwise or clockwise, degree angle.



3. Position Adjustment

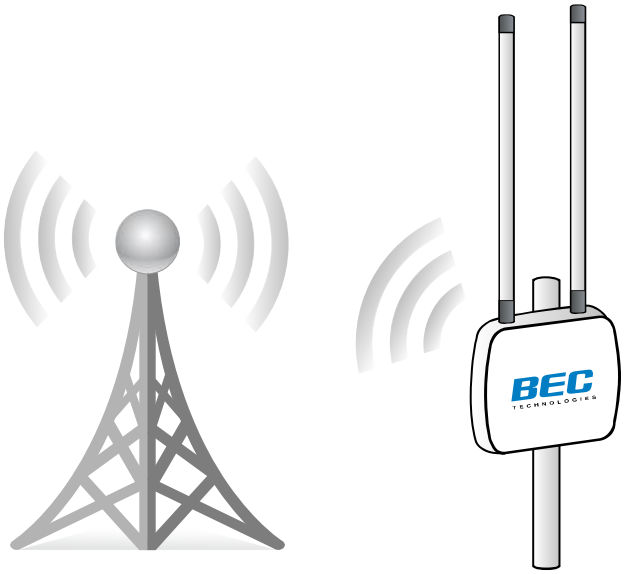
3.1 Using an Embedded Directional Antenna

3.1.1 Find the location and best angle for getting the strongest signal from the base station. The CPE must be directed towards the nearest base station.

3.3.2 Adjusting CPE position to get a better reception and/or fine-tuning the CPE orientation (in horizontal/vertical position or 45 degree angle position) to have the best signal strength

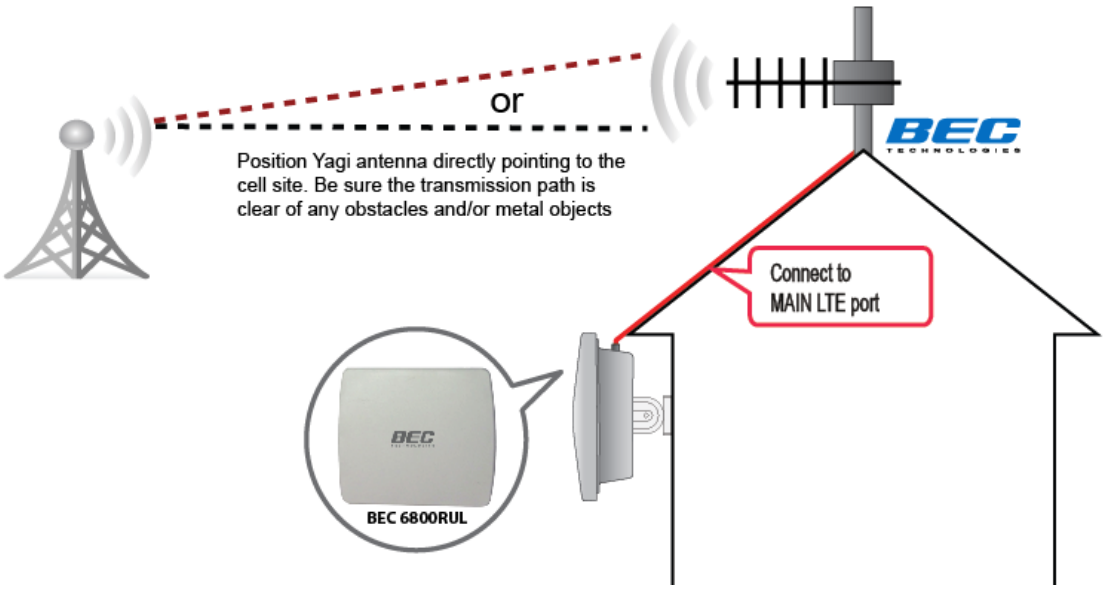
3.2 Using two (2) Omni Directional Antennas

3.2.1 Find the location and best angle for getting the strongest signal from the base station. The CPE must be directed towards the nearest base station.



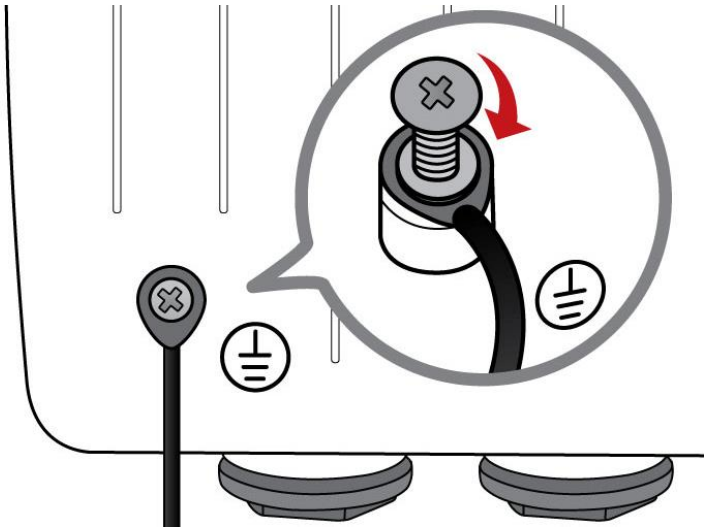
3.3 Using an External Yagi Antenna

Find a good spot to mount the Yagi antenna, such as a chimney or rooftop, to avoid trees, building, and any metal objects. The Yagi antenna must be directly pointing to the nearest base station for strongest signals.


or
Position Yagi antenna directly pointing to the cell site. Be sure the transmission path is clear of any obstacles and/or metal objects
BEC
Connect to MAIN LTE port
BEC
BEC 6800RUL

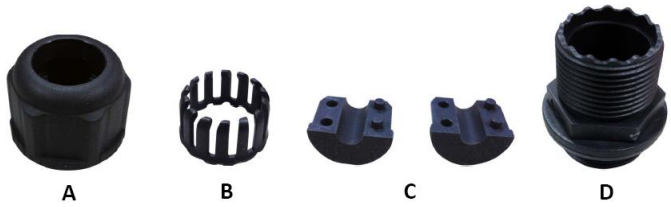
4. Grounding the CPE to Complete the Installation

Attach the grounding wire to the CPE and tighten the screw

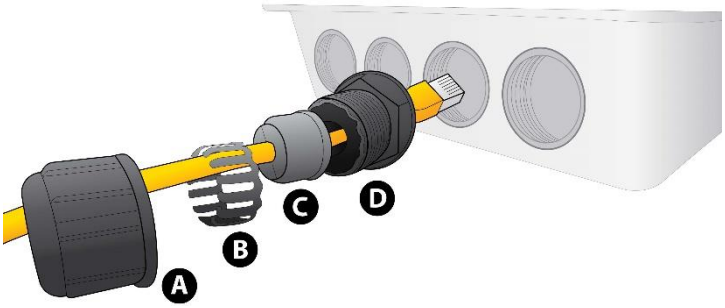


5. Power on your LTE router

Step 1: Assemble M25 cable gland



Step 2: Unscrew the LAN (PoE) port and insert the supplied outdoor Ethernet cable (RJ-45) through material A-D, and then connect the RJ-45 Ethernet cable into the CPE port.



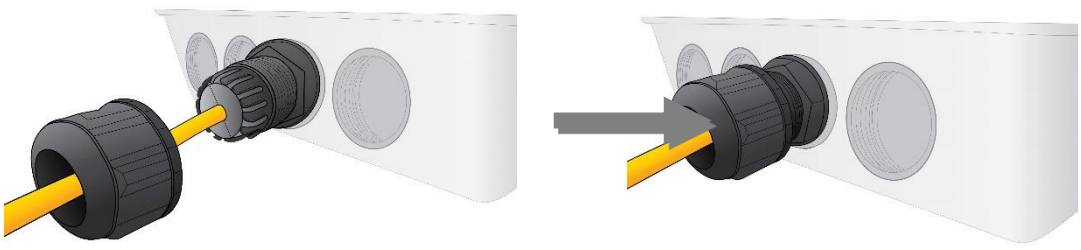
Step 3:

3.1: Insert Ⓒ at the back end of Ⓓ

3.2: clip Ⓑ on Ⓒ

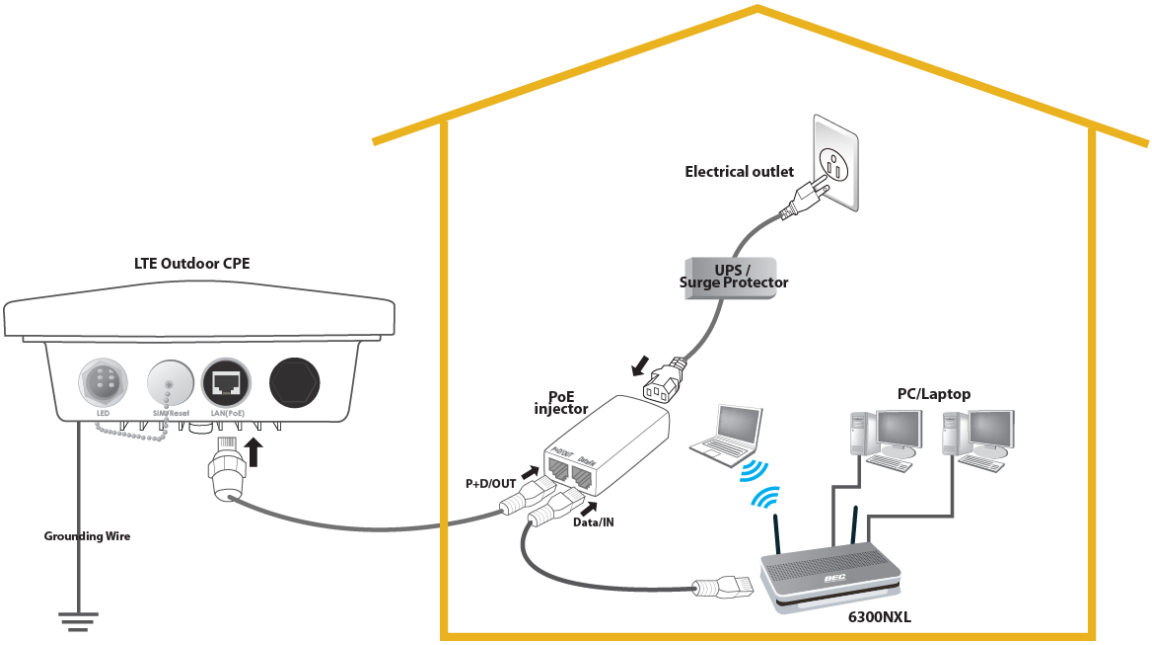
3.3: keep Ⓑ close to Ⓓ

3.4: then tighten Ⓐ.



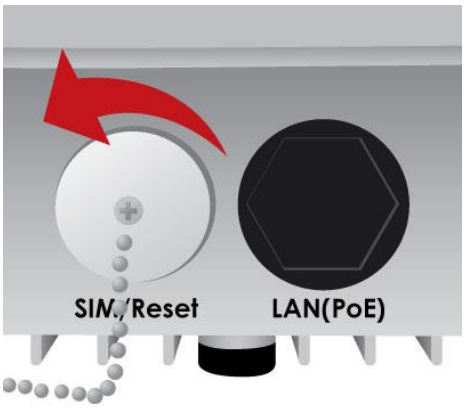
Step 4: Insert the other end of outdoor Ethernet cable (RJ-45) to the supplied PoE injector **P+D/OUT** port. Connect another Ethernet cable (RJ-45) directly to the **Data/IN** port and the other end of cable to a switch or broadband router. Plug the PoE power cable to an electrical outlet to power on your LTE router.

IMPORTANT: It is recommended to put the PoE Injector on an UPS or Surge Protector. Use the supplied grounding wire to ground your 6800RUL ODU is REQUIRED!



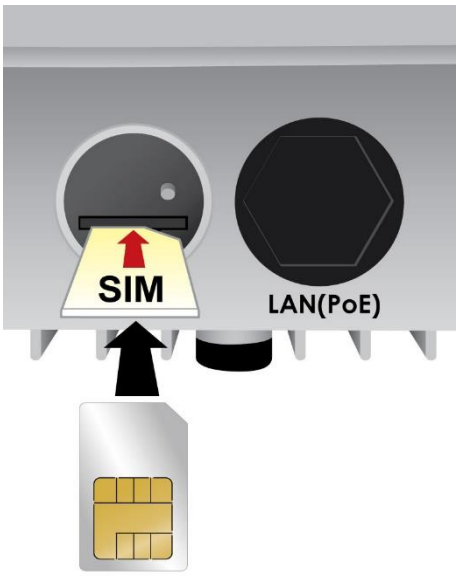
6. Set up your LTE Internet Connection

Step 1: Unscrew the cap of SIM card slot.

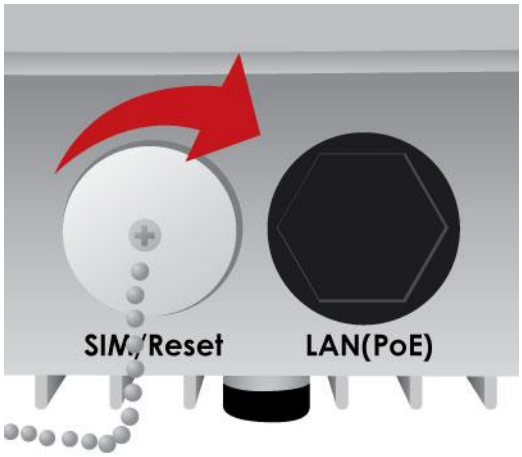


Step 2: Slide the SIM card into the card slot of the device. Make sure that the SIM card is slid into the bottom of the slot with a click.

IMPORTANT: It is recommended to use an industrial grade SIM card.



Step 3: Screw the cap back tightly.



Warning

Please power off the device before inserting or removing the SIM card.

CHAPTER 3: BASIC INSTALLATION

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98 / NT /2000 / XP / ME / 7 / Vista, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed or configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

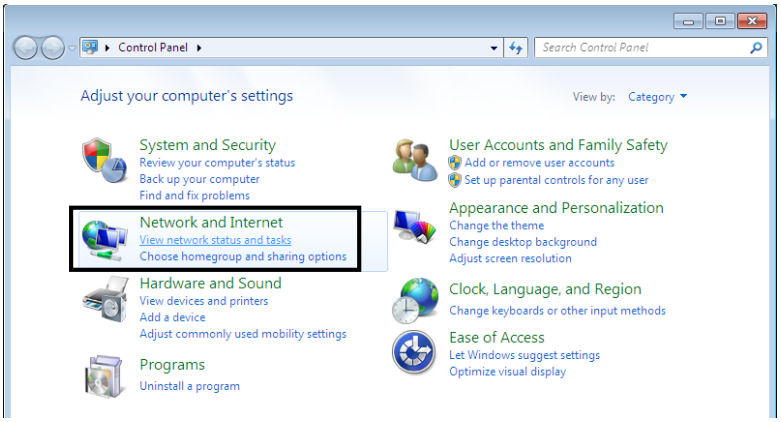
Any TCP/IP capable workstation can be used to communicate with or through the **BEC 6800RUL**. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

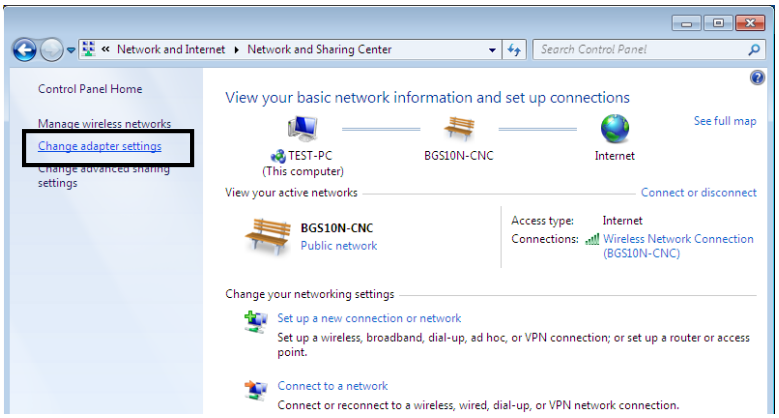
Configuring PC in Windows 7 (IPv4)

1. Go to **Start**. Click on **Control Panel**.

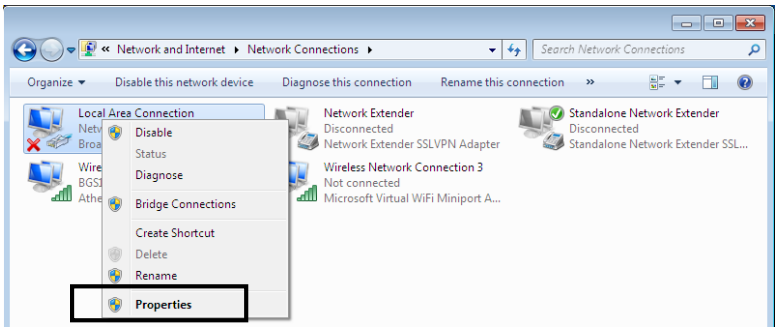
2. Then click on **Network and Internet**.



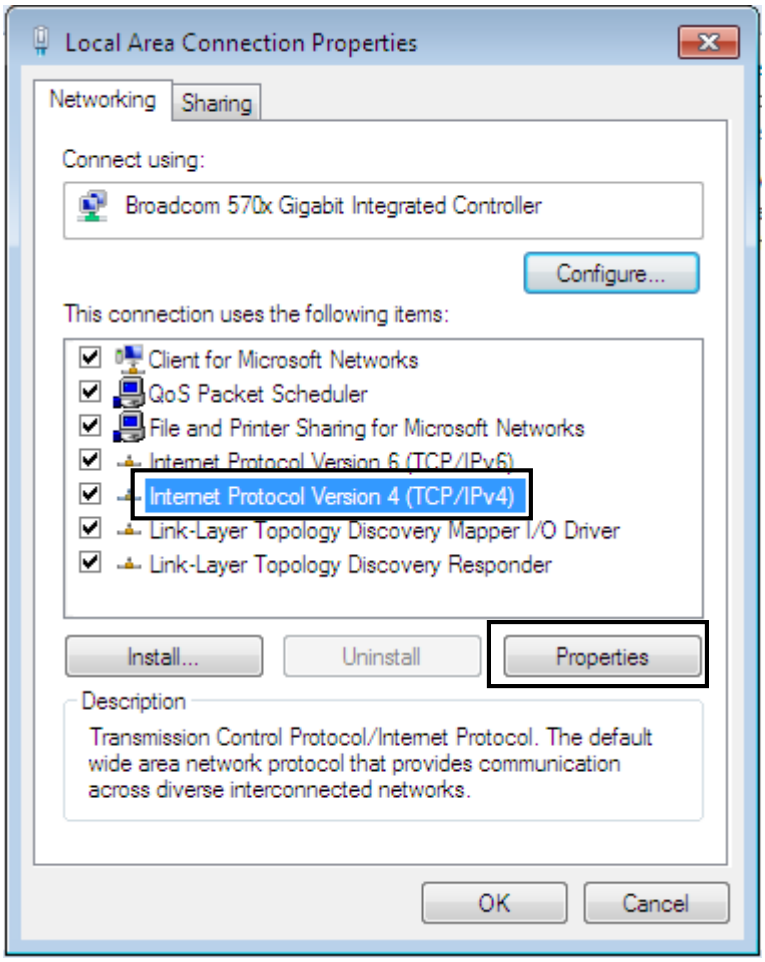
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet
Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

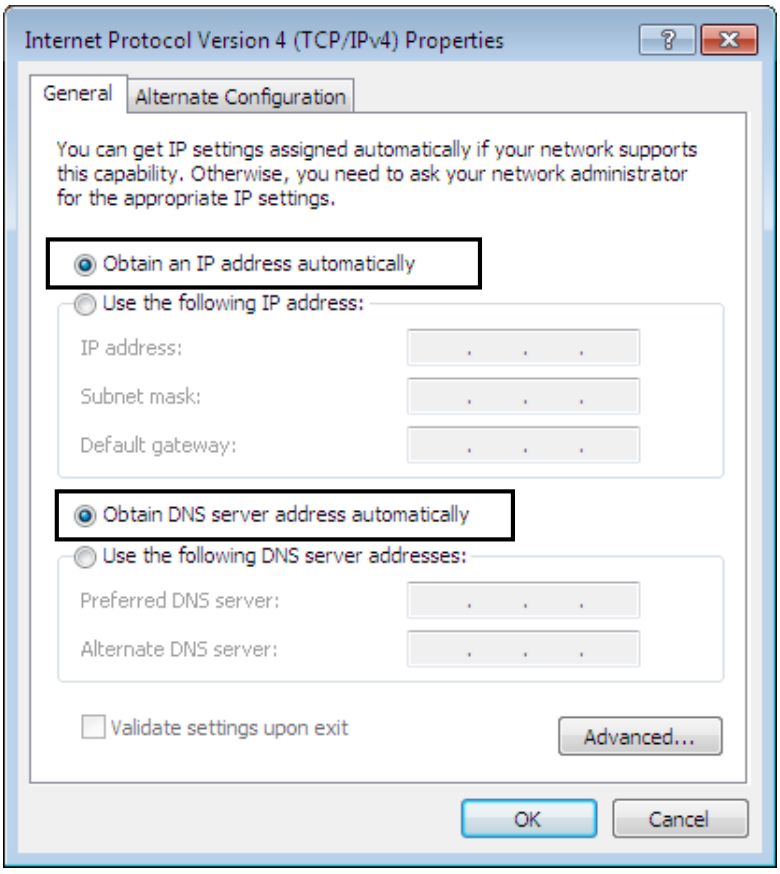


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

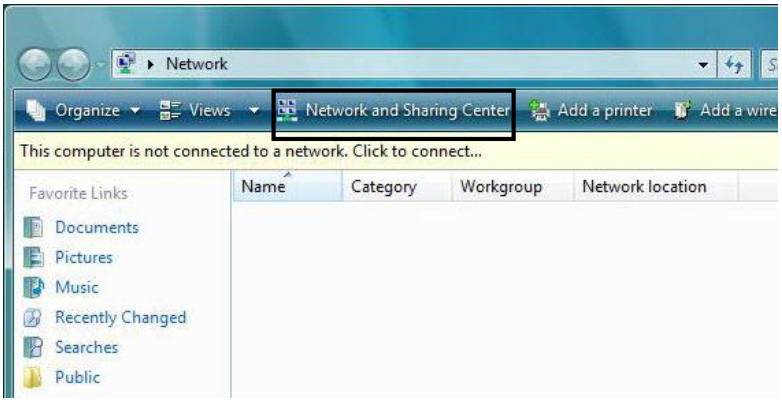
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

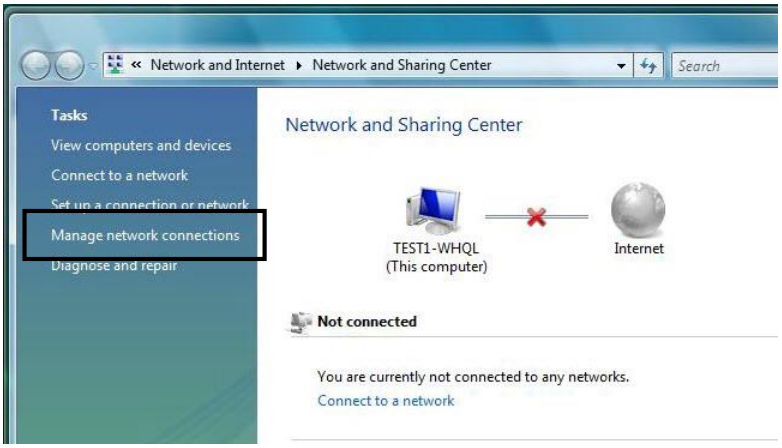
Configuring PC in Windows Vista (IPv4)

1. Go to **Start**. Click on **Network**.

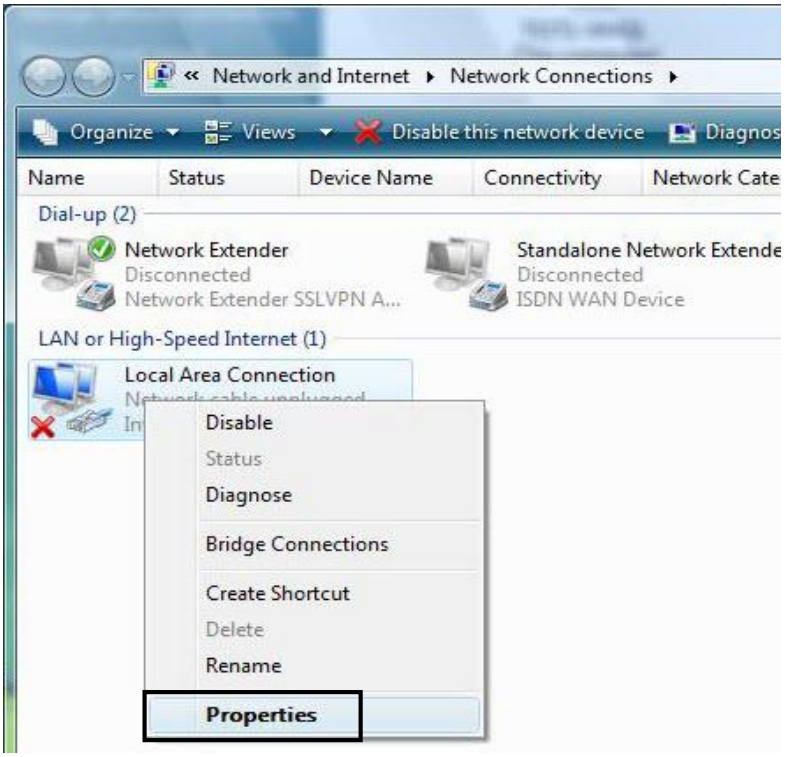
2. Then click on **Network and Sharing Center** at the top bar.



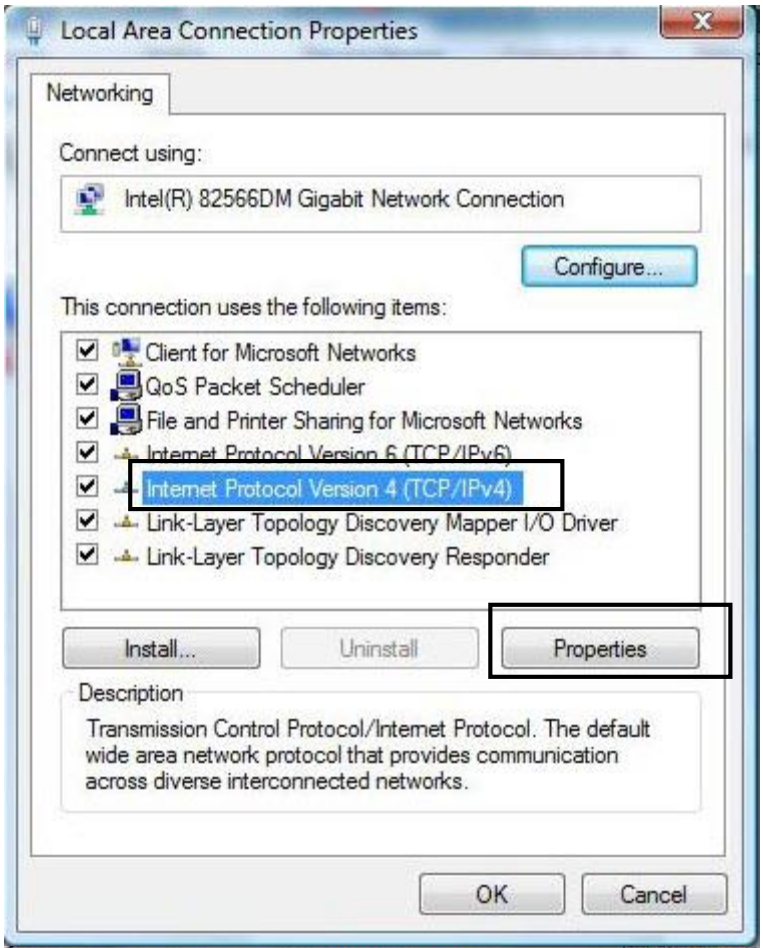
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

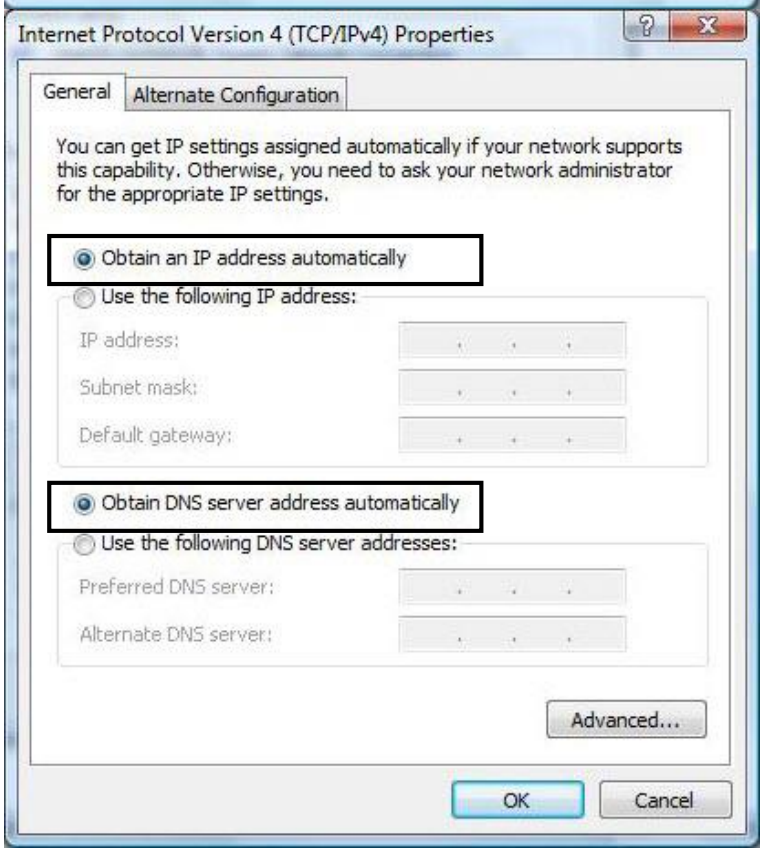


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



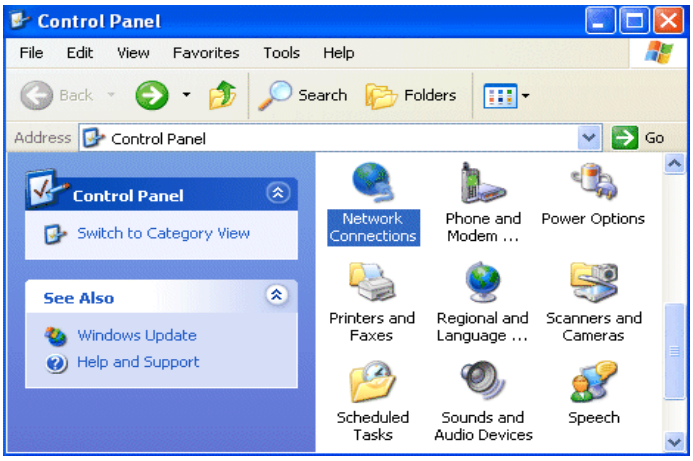
6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

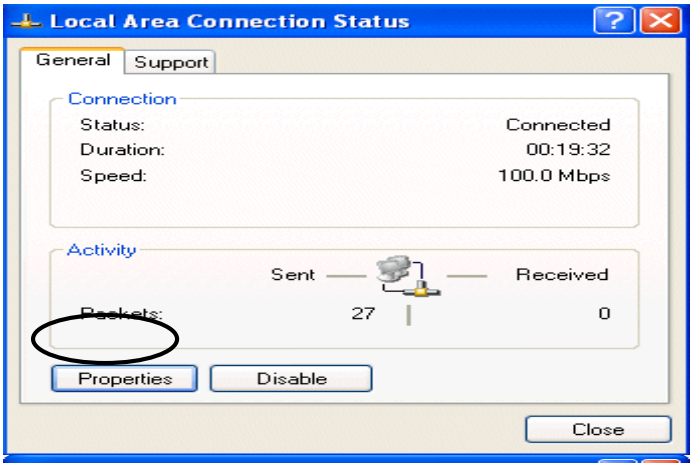

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows XP (IPv4)

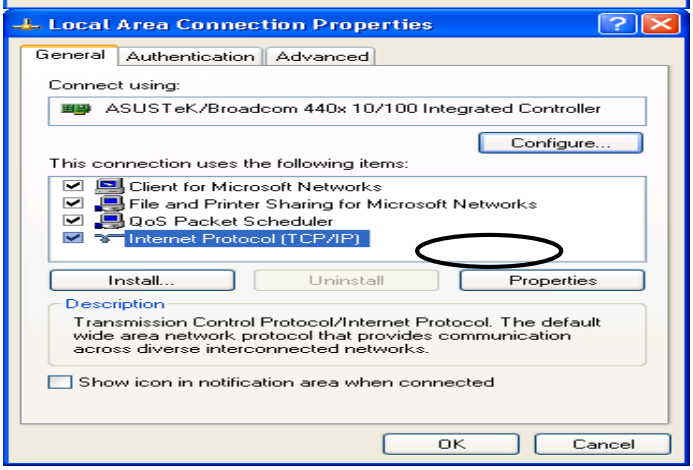
1. Go to **Start**. Click on **Control Panel.**
2. Then click on **Network and Internet**.



3. In the **Local Area Connection Status** window, click **Properties**.

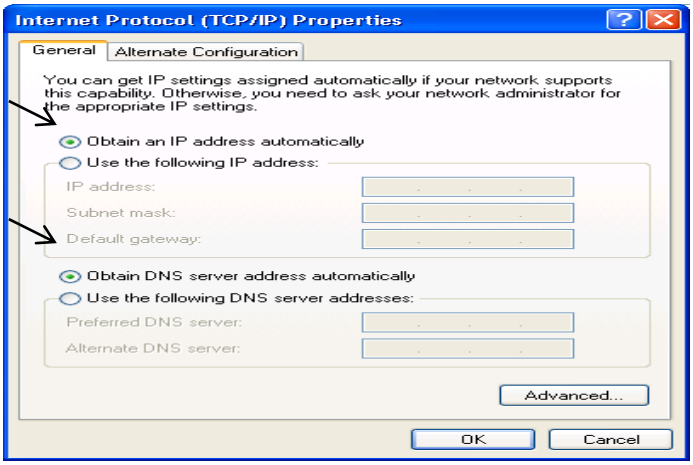


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.


Local Area Connection Properties
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

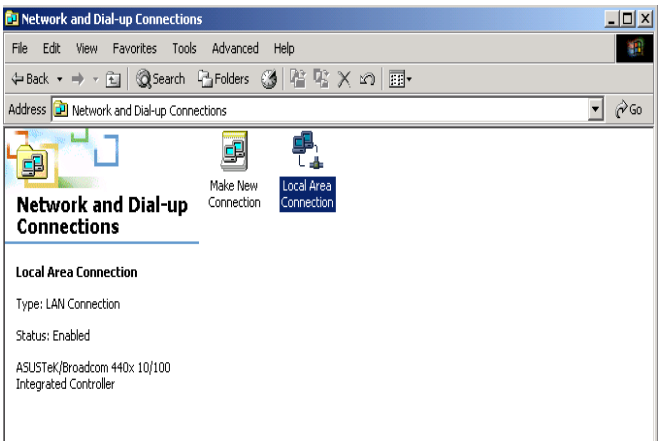
6. Click **OK** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

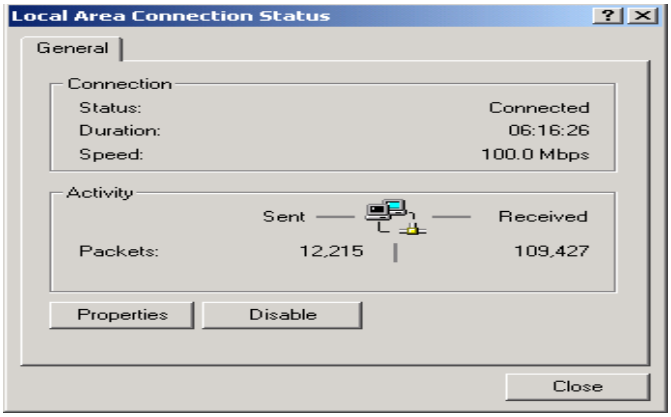
Configuring PC in Windows 2000 (IPv4)

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

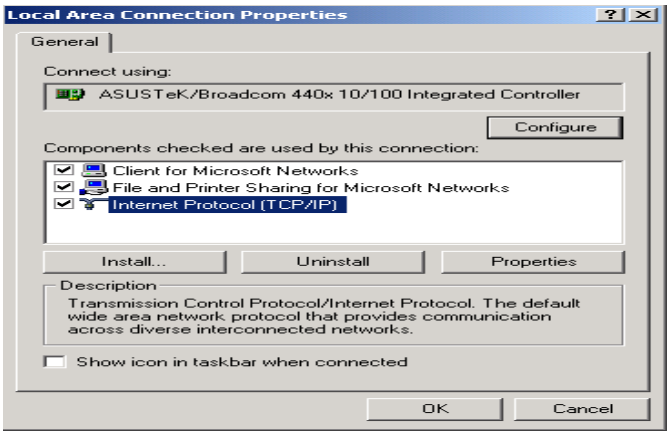
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window click **Properties**.

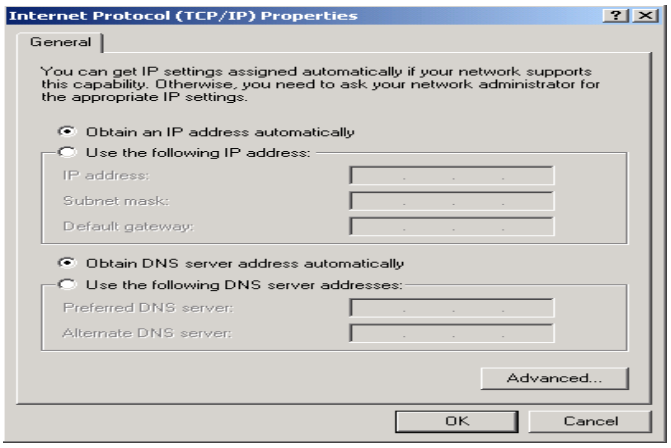


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

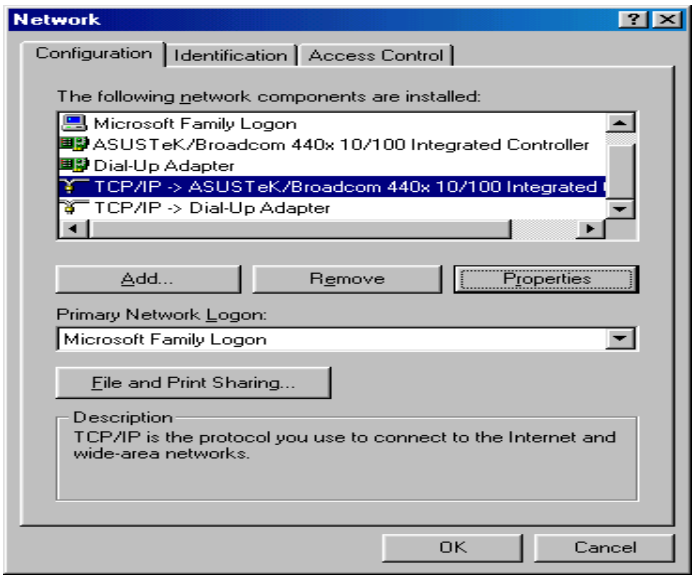
6. Click **OK** to finish the configuration.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

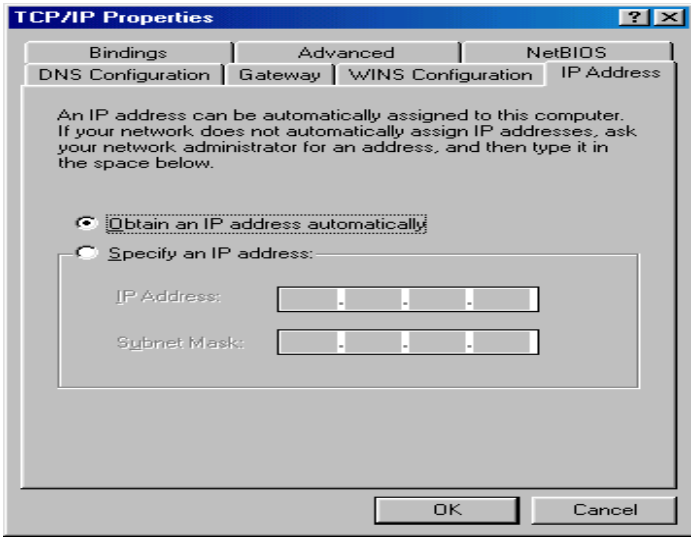
Configuring PC in Windows 98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.

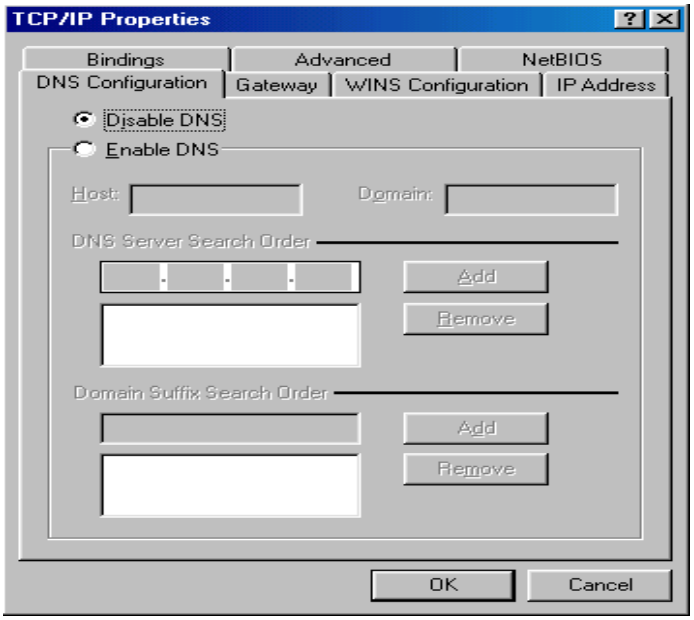


3. Select the **Obtain an IP address automatically** radio button.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

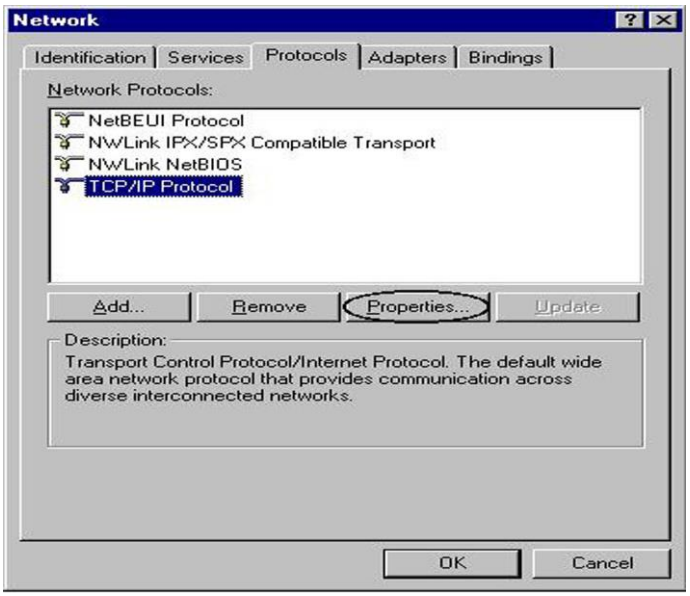
4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



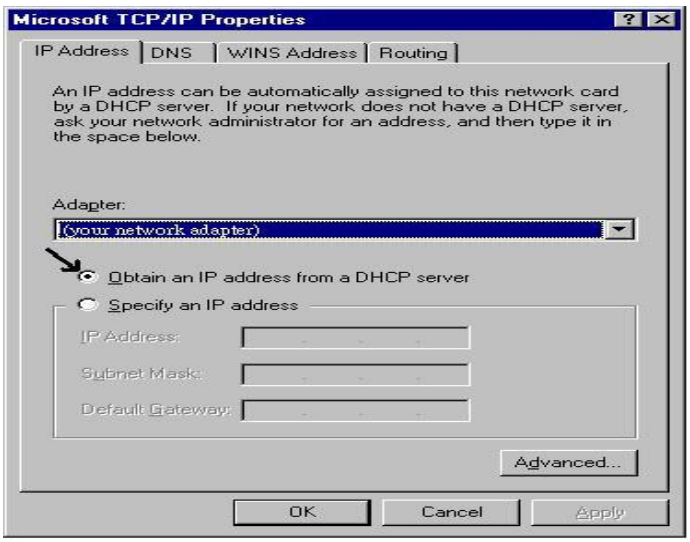
Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.



2. Select **TCP/IP Protocol** and click **Properties**.

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.

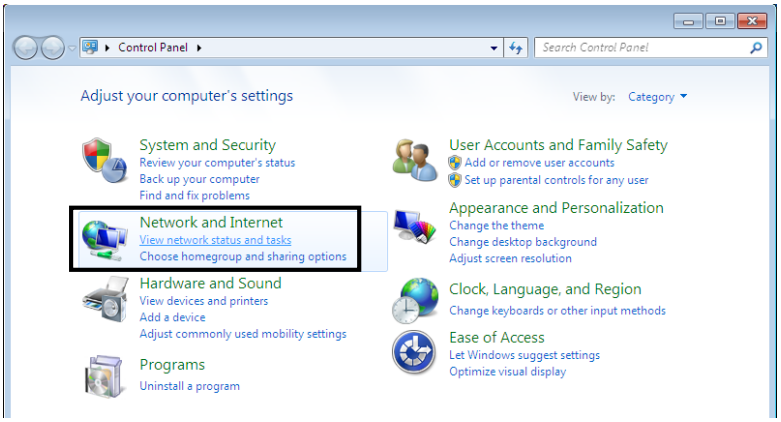

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Network Configuration – IPv6

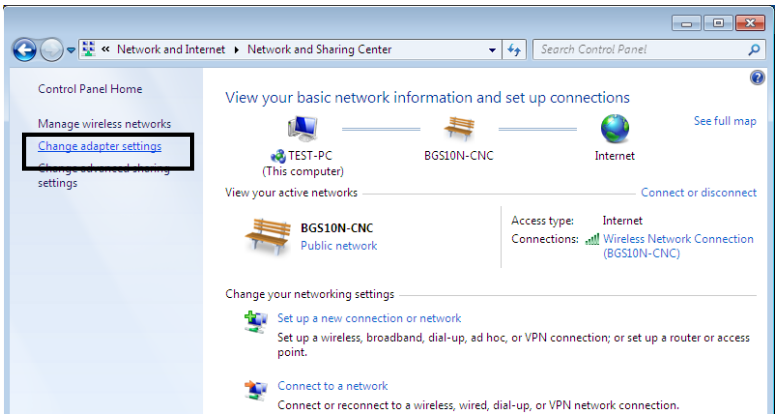
Configuring PC in Windows 7 (IPv6)

1. Go to **Start**. Click on **Control Panel**.

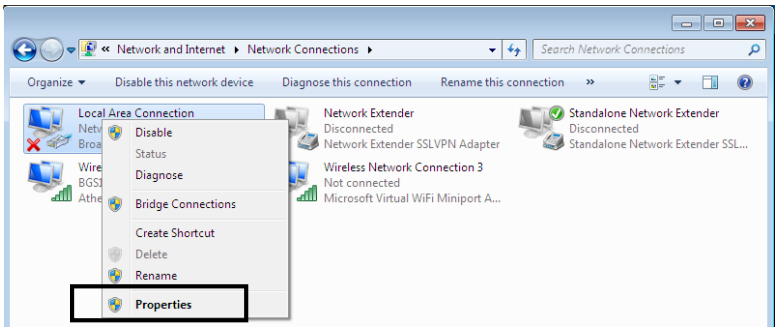
2. Then click on **Network and Internet**.



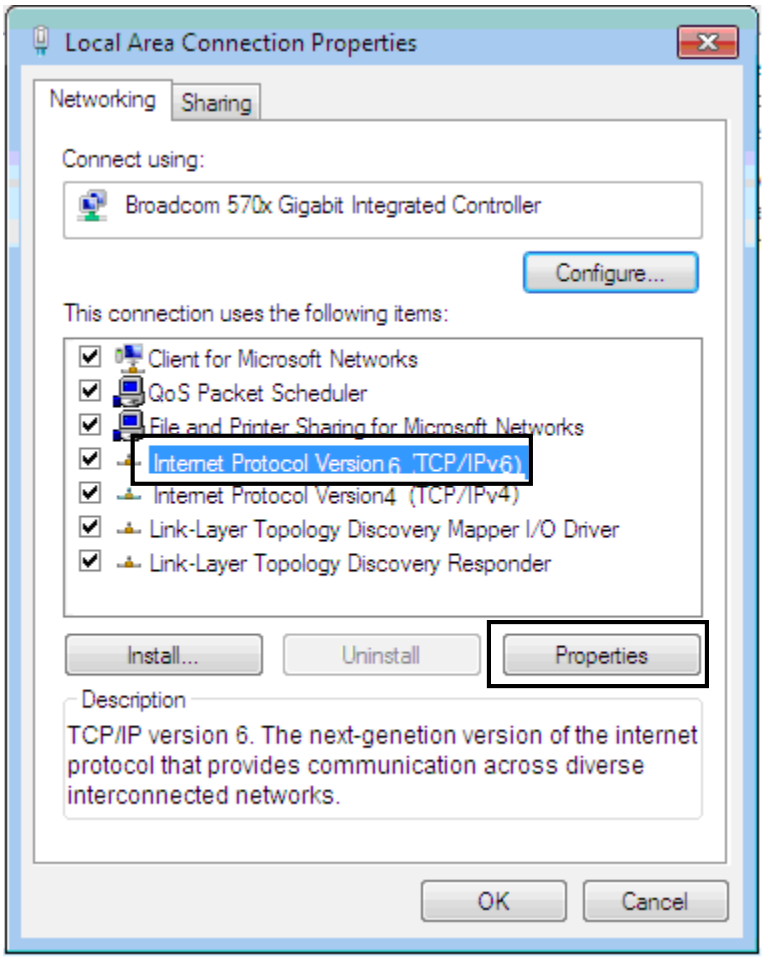
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet
Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

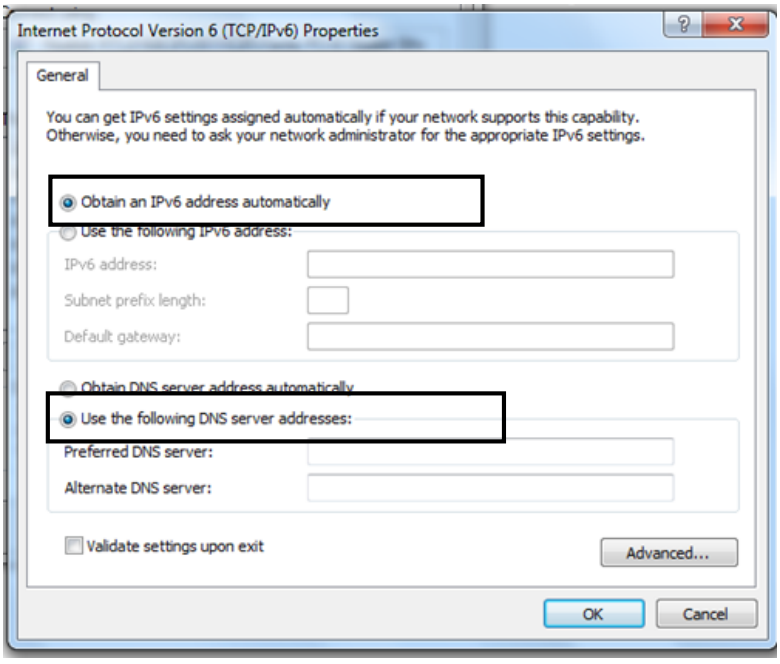


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

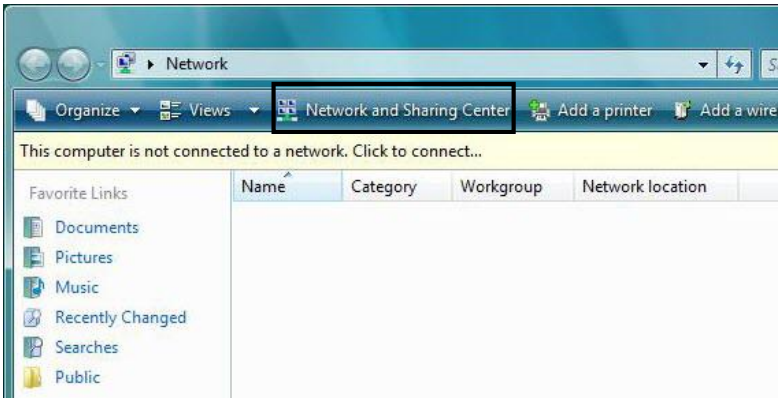
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.


Internet Protocol Version 6 (TCP/IPv6) Properties
General
You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.
Obtain an IPv6 address automatically
Use the following IPv6 address:
IPv6 address:
Subnet prefix length:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

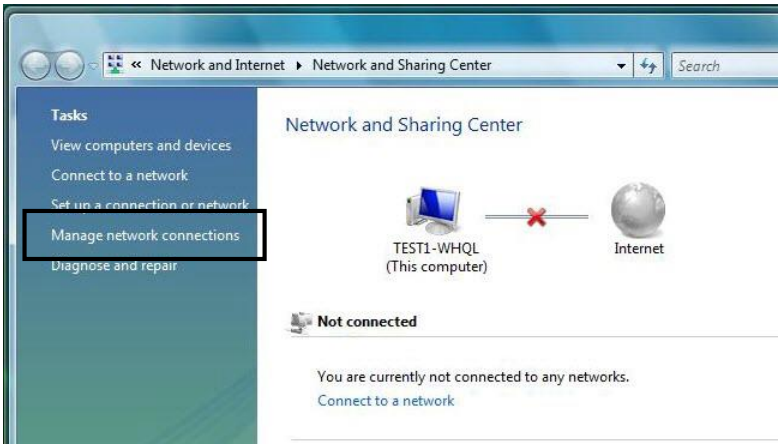
Configuring PC in Windows Vista (IPv6)

1. Go to **Start**. Click on **Network**.

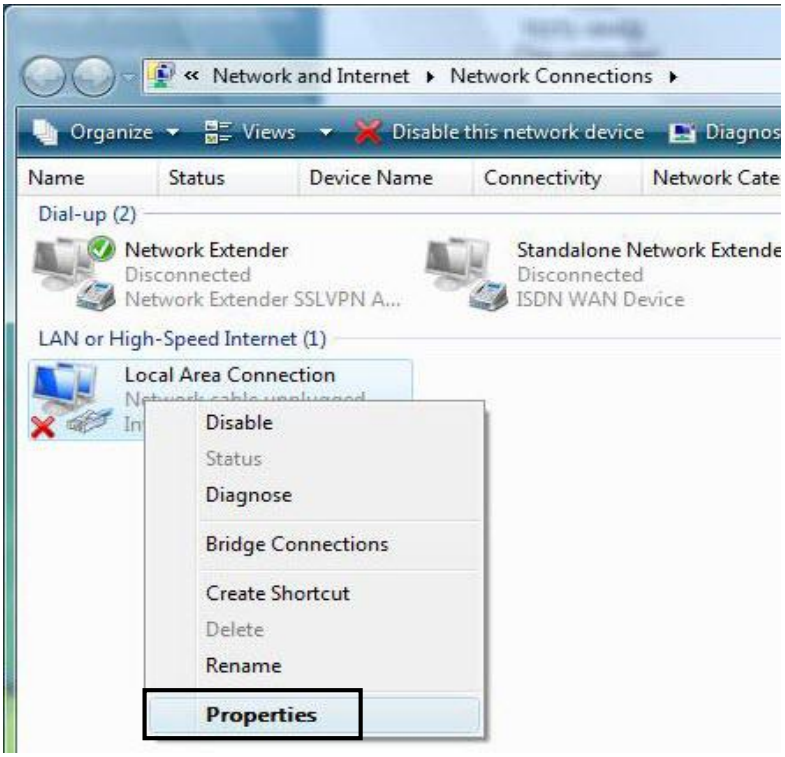
2. Then click on **Network and Sharing Center** at the top bar.



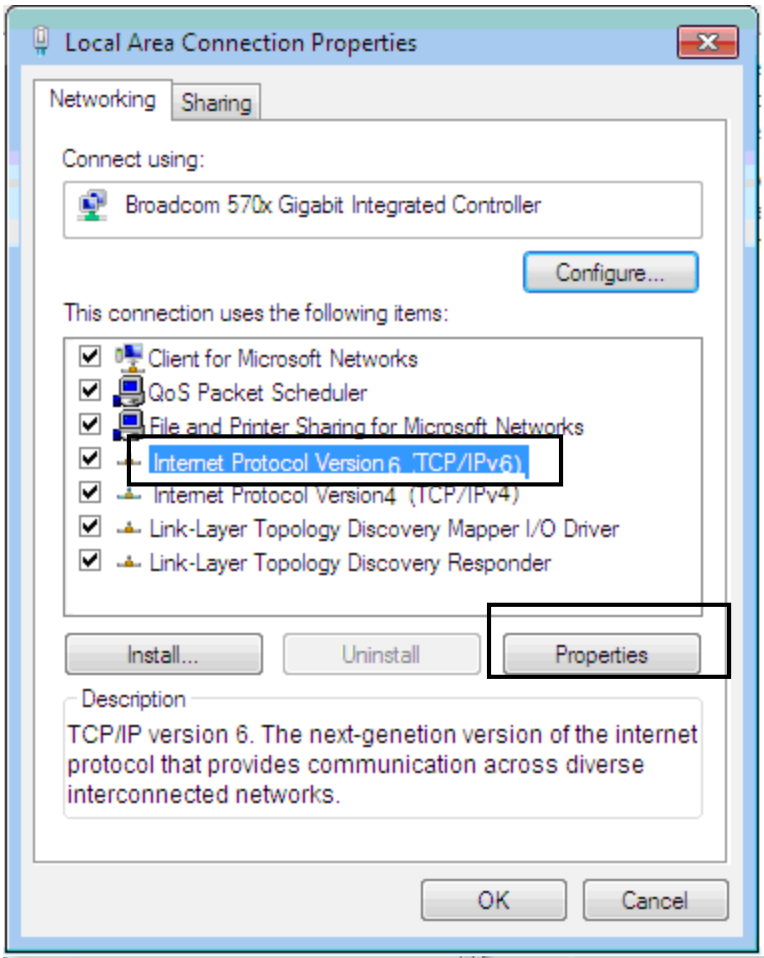
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

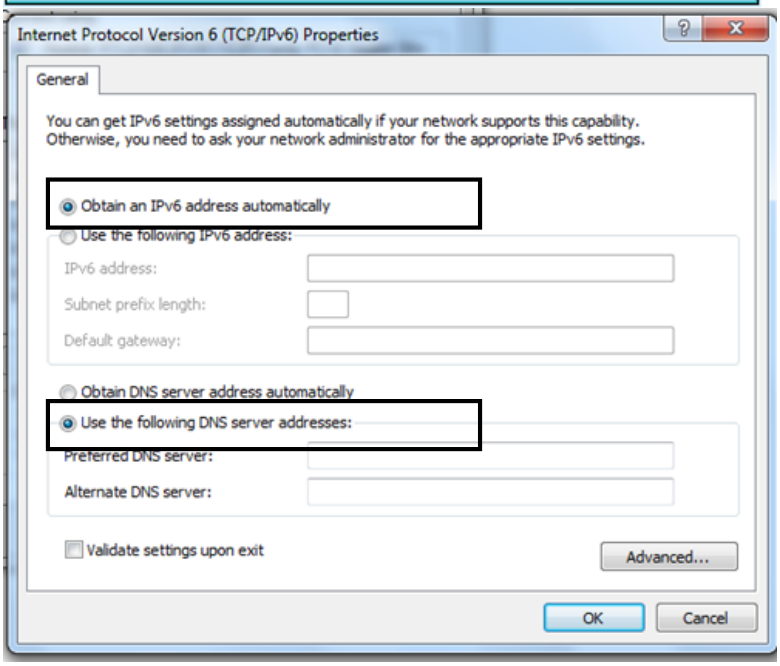


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

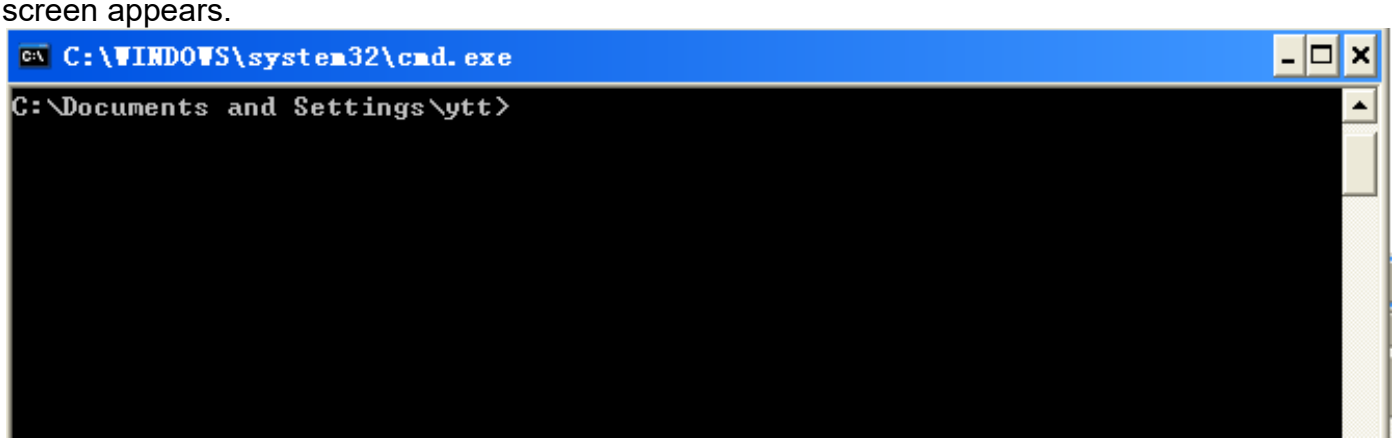

Internet Protocol Version 6 (TCP/IPv6) Properties
General
You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.
Obtain an IPv6 address automatically
Use the following IPv6 address:
IPv6 address:
Subnet prefix length:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Configuring PC in Windows XP (IPv6)

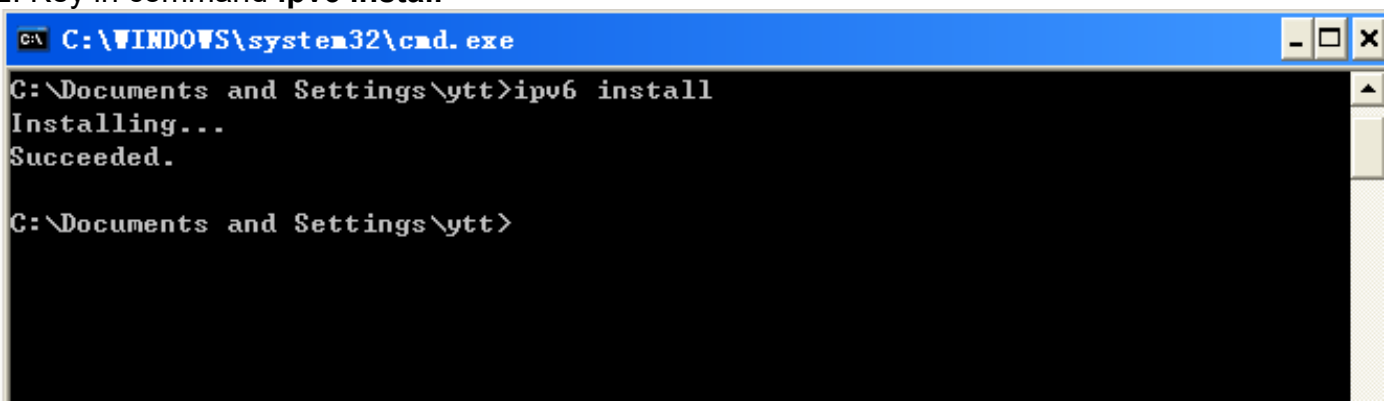
IPv6 is supported by Windows XP, but you need to install it first.

Please follow the steps to install IPv6:

1. On the Desktop, Click **Start** > **Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.



2. Key in command **ipv6 install**



Installation of IPv6 is now completed. Please test it to see if it works or not. .

Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

- ✔ Username: admin
- ✔ Password: admin

The default username and password are "**admin**" and "**admin**" respectively.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.
Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

- ✔ IP Address: 192.168.1.254
- ✔ Subnet Mask: 255.255.255.0

DHCP Server:

- ✔ DHCP server is enabled.
- ✔ Start IP Address: 192.168.1.100
- ✔ IP pool counts: 100

CHAPTER 4: BASIC CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password window prompt appears. Enter the user name and password that your administrator has set for you and select the **Account Type**, then click **Login**.

The default username and password is **"admin"** and **"admin"** respectively for the **Administrator** account type.

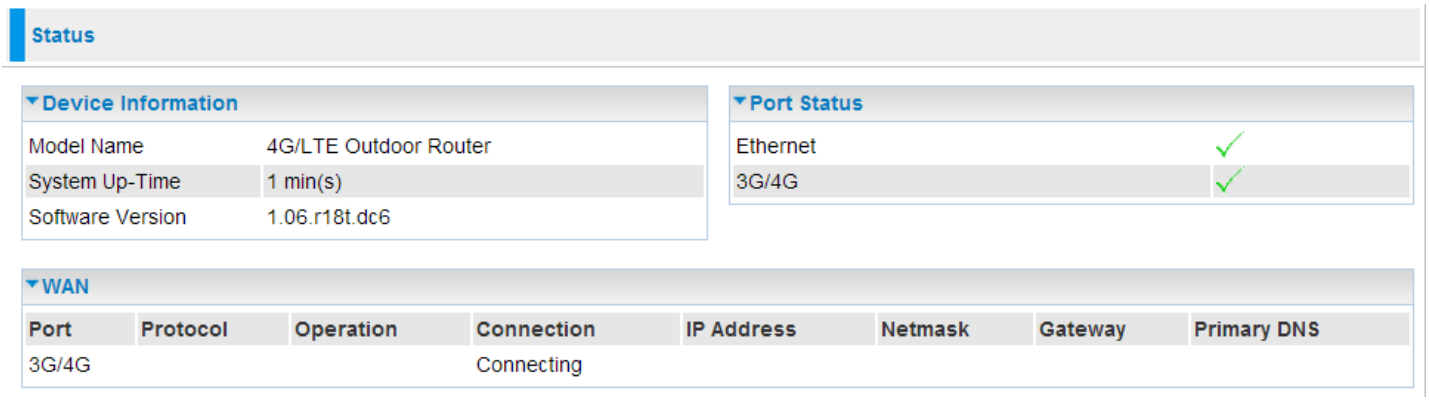
NOTE: This username / password may vary by different Internet Service Providers.

Congratulations! You have successfully logged on to your **BEC 6800RUL.**

Once you have logged on to your router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

- **Advanced** (Click to switch to the Advanced Configuration Mode)
- **Status**
- **Quick Start**
- **WAN**

Status



Device Information

Model Name: Provide a name for the router for identification purposes.

System Up-Time: Record system up-time.

Software Version: Firmware version.

Port Status

Port Status：User can look up to see if they are connected to Ethernet and 3G / 4G_LTE

WAN

Port: Name of the WAN connection.

Protocol: PPPoE, Dynamic or Fixed for WAN

Operation: Current available operation.

Connection: The current connection status.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

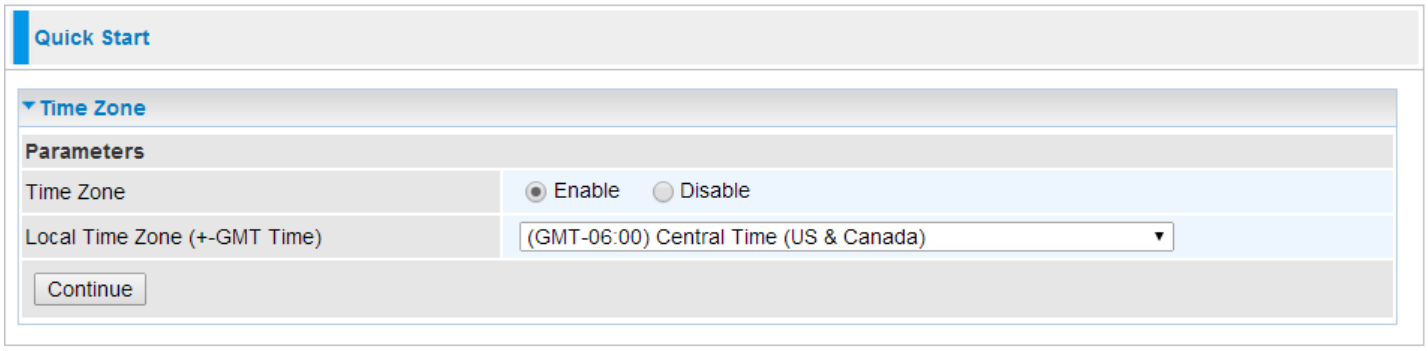
Primary DNS: The IP address of the primary DNS server.

Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup time zone and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

Step 1 – Time Zone

Enable and Select the appropriate Time Zone, then click **Continue** to go on to next step. You can turn **Time Zone** to understand more.

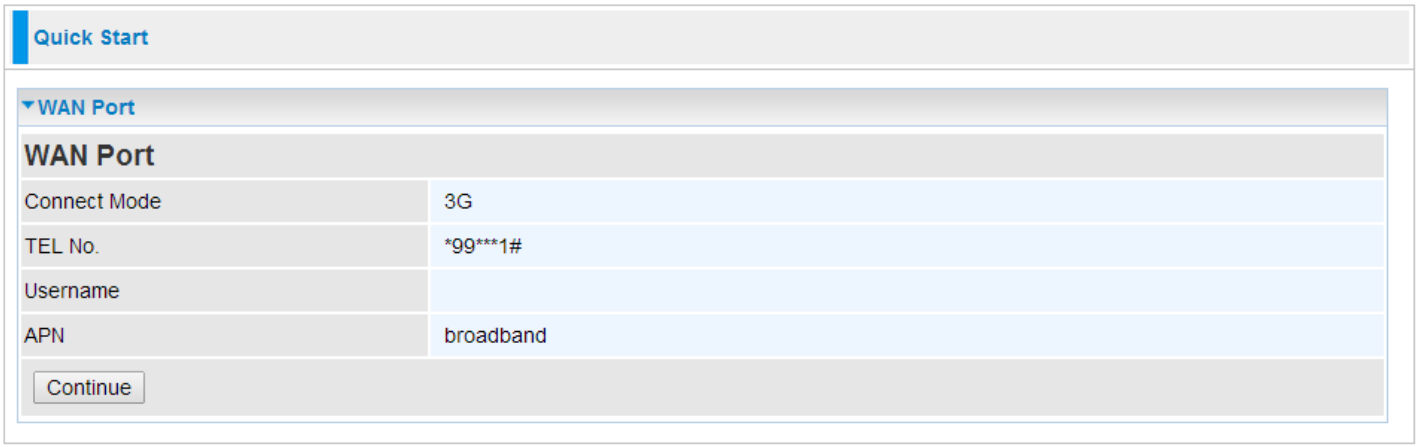


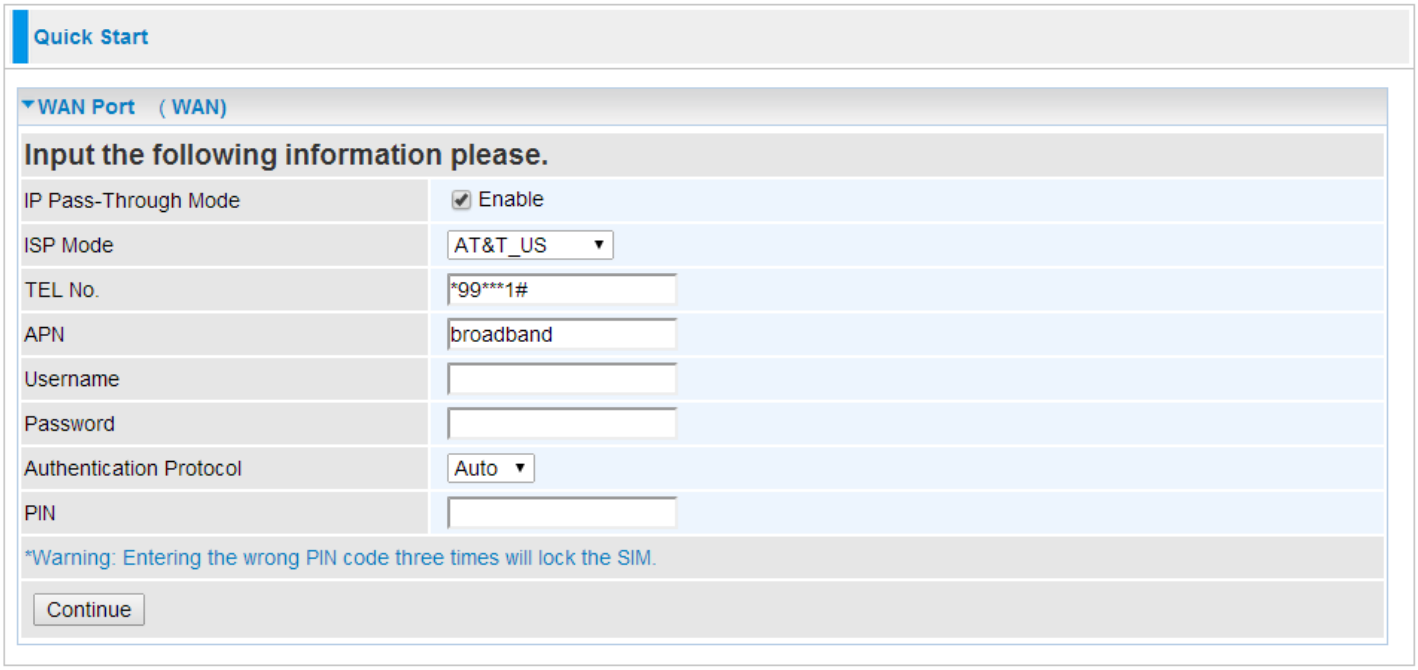
Step 2 – WAN

Click **Continue** to enter your SIM card inform for registration.

Enter your SIM card telephone number, APN, Username, Password, PIN, etc.

If you have trouble to find these information, please consult with your SIM carrier.





Note: when re-inserting the 3G / 4G SIM card to the BEC 6800RUL, you should again press Continue button to make 3G / 4G connection take effort, or you can Save Config and Restart the router to reach the same effort.

Step 3 – Configuration in Process

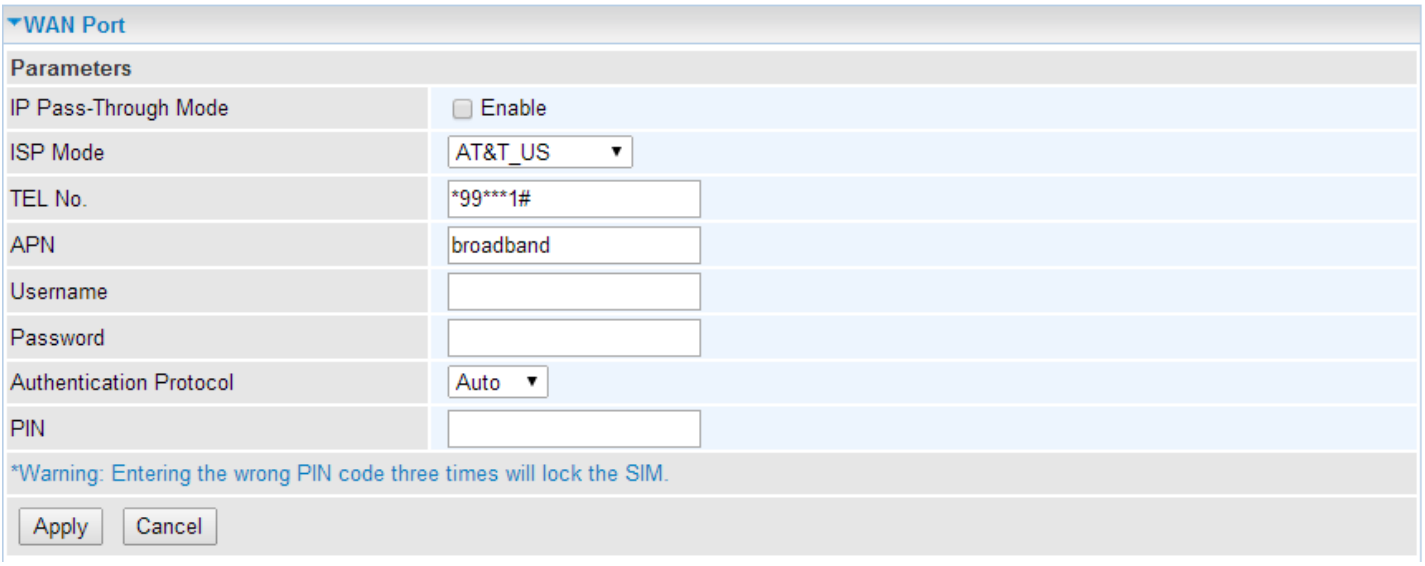
The 6800RUL will take 15~30 seconds to configure the settings. Once it is done, you will see a "Configurations!" window.

Step 4 – Quick Start Completed!

You now may be able to access to the Internet. If not, please check your WAN, Internet Connection, setup again.

To review the WAN connection, please go back to **Status** for more information.

WAN



IP Pass-through Mode: When **enabled**, BEC 6800RUL is in bridge mode that it does not obtain a WAN IP address; features such as routing capabilities, NAT, firewall, etc., are being disabled. The client router that is behind the BEC 6800RUL now obtains a WAN IP address. When **disabled**, BEC 6800RUL is in router mode that it handles a WAN IP address and all features are become available.

ISP Mode: A list of 3G / 4G service providers that is available.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS / LTE call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G / 4G operators use the APN 'internet' for their portal. The default value of APN is "broadband".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

NOTE: when the 3G / 4G SIM card is pulled out and then insert into again, you should again press Apply button to make 3G / 4G connection take effort, or you can Save config and Restart the route to reach the same effort.

CHAPTER 5: ADVANCED CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click "**Go**", a user name and password window prompt appears. Enter the user name and password that your administrator has set for you and select the **Account Type**, then click **Login**.

The default username and password is **"admin"** and **"admin"** respectively for the **Administrator** account type.

NOTE: This username / password may vary by different Internet Service Providers.

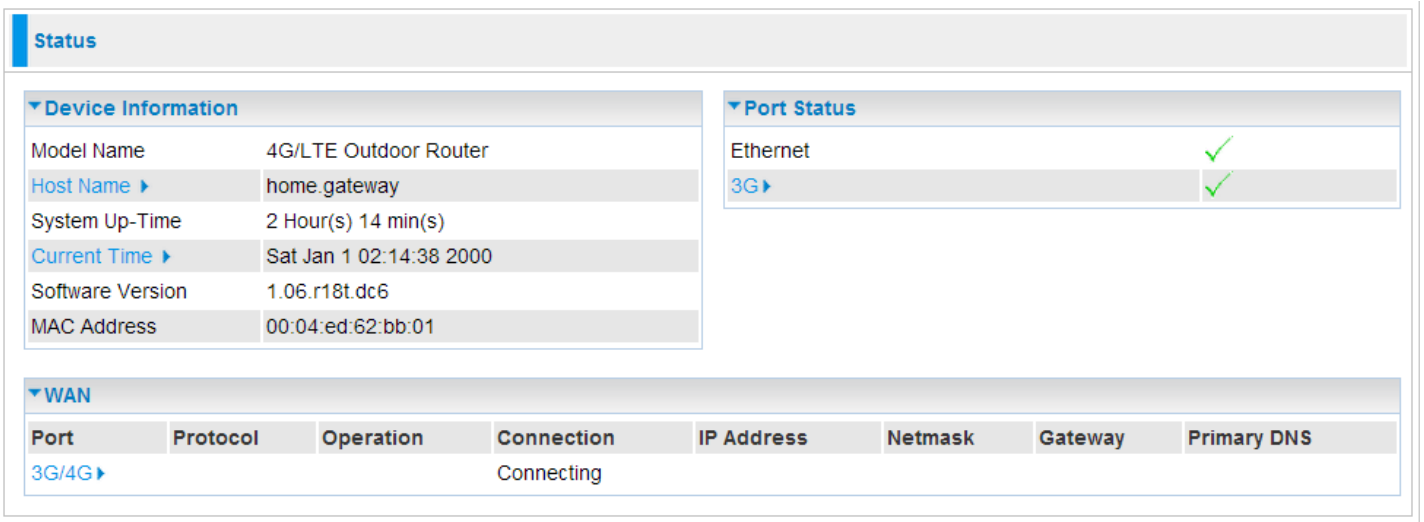
Congratulations! You have successfully logged on to your **BEC 6800RUL.**

Once you have logged on to your BEC 6800RUL via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation panel links you directly to each feature contents, which include:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	**Mobile Status**		**LAN** - Ethernet - IP Alias - DHCP Server
	ARP Table		**WAN** - WAN Profile
	DHCP Table		**System** - Time Zone - Firmware Upgrade - Backup / Restore - Restart - User Management - Mail Alert
	System Log		**Firewall** - Packet Filter - MAC Filter - Intrusion Detection - Block WAN Ping - URL Filter
	Firewall Log		**QoS**
	UPnP Portmap		**Virtual Server** - Port Mapping - DMZ
			Time Schedule
			Advanced - Static Route - Static ARP - Dynamic DNS - Device Management - SIP_ALG - IGMP - SNMP Access Control - TR-069 Client - Remote Access

The following sections provide details explanation and configuration of the settings available in the **BEC 6800RUL** router.

Status



Device Information

Model Name: Display the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name. Click this link to turn to **Device Management** configuration.

System Up-Time: Record system up-time.

Current time: Set the current time. See the Time Zone section for more information. Click this link to turn to **Time Zone** configuration.

Software Version: Firmware version.

MAC Address: The LAN MAC address.

Port Status

Port Status：Display available connection interfaces that are supported in the BEC 6800RUL. Users can look up the status of each interface.

WAN

Port: List current available WAN connections.

Operation: Current available operation.

Connection: The current connection status.

IP Address: WAN port IP address.

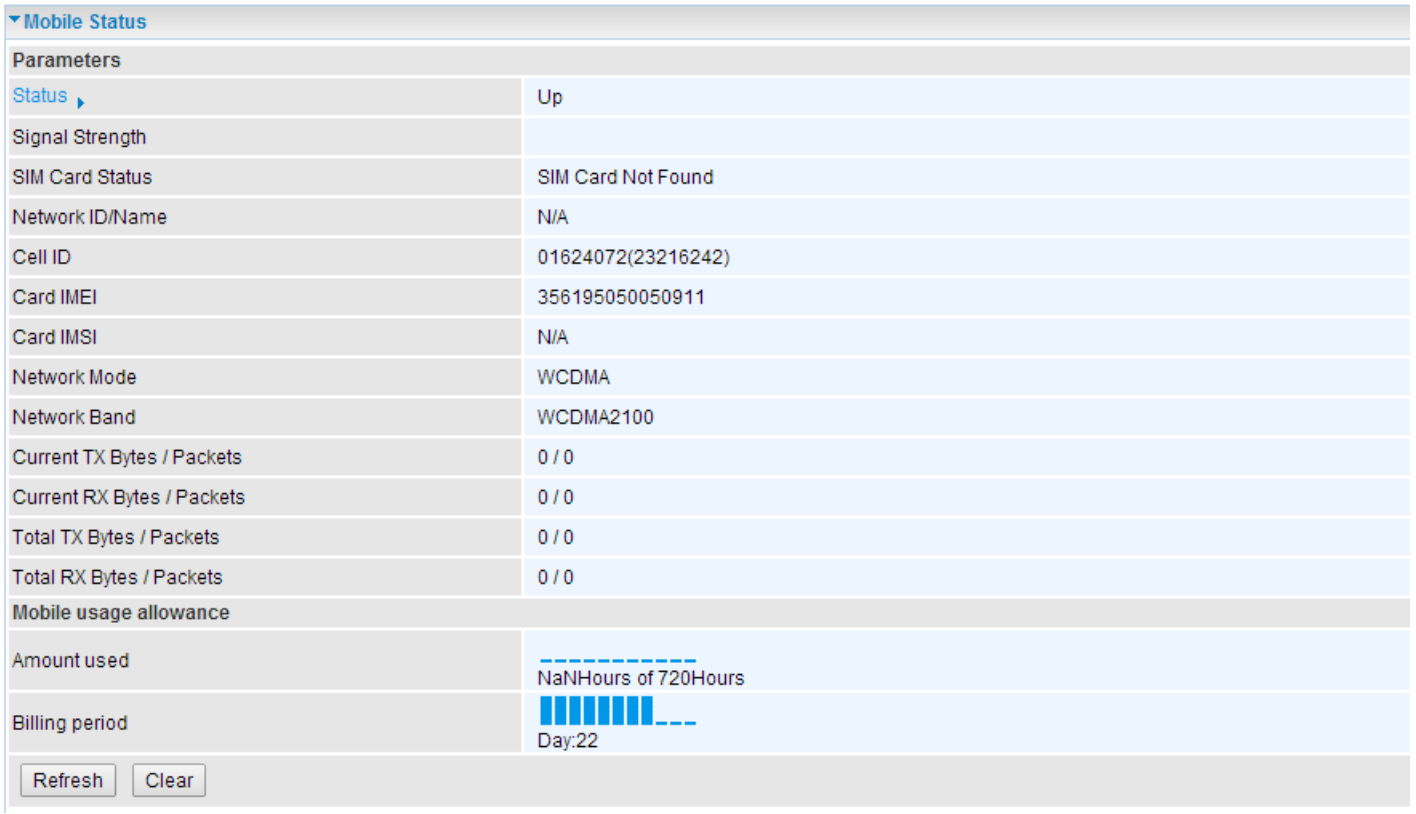
Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

Mobile Status

This section displays the 3G / 4G Card overall status with information such as the current signal strength, statistics of current data transmission and total data transmission.



Status: The current status of the 3G/4G-LTE connection.

Signal Strength: The signal strength bar indicates the current 3G/4G signal strength.

SIM Card Status: It indicates if the SIM Card is being inserted correctly or not. If SIM card is not installed properly or cannot be detected, “SIM Card Not Found” will be displayed.

Network ID / Name: The network ID and/or name that the SIM card is connected to.

Cell ID: The information of Cell ID.

Card IMEI: The unique identification number that is used to identify the 3G / 4G card.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G / 4G card

Network Mode: Show the using network mode.

Network Band: Show the using network band.

Current TX Bytes / Packets: The statistics of data transmission in bytes / packets during a call.

Current RX Bytes / Packets: The statistics of data received in bytes / packets during a call.

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

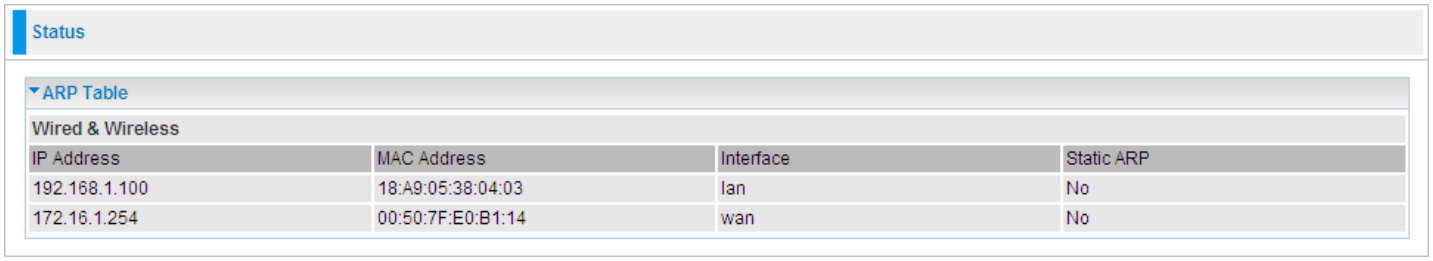
Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

Amount used: Show the traffic or hours has been used.

Billing period: The day from which the fee is charged.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall / MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



IP Address: It is IP Address of internal host that join this network.

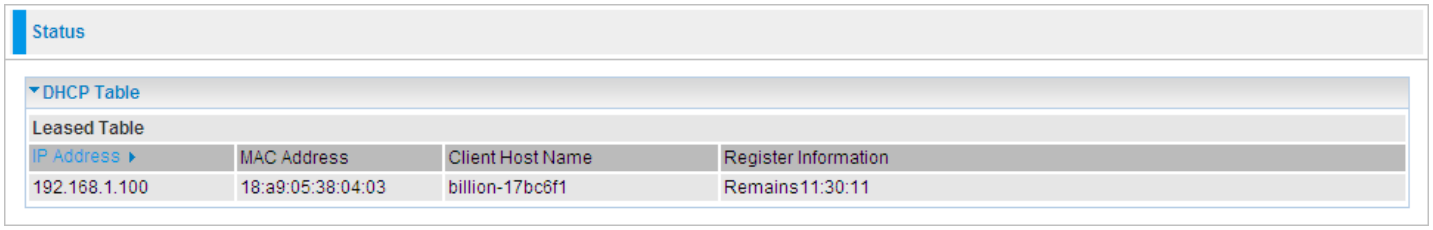
MAC Address: The MAC address of internal host.

Interface: indicates which side the IP addresses locate on. WAN means the corresponding IP locates on WAN side.

Static ARP: The state for ARP.

- **"No"** for dynamically-generated ARP table entries.
- **"Yes"** for static ARP table entries added by the user.

DHCP Table



IP Address: The current corresponding DHCP-assigned dynamic IP address of the device. Click this link to configure DHCP Server, for more information, turn to Page 63-64.

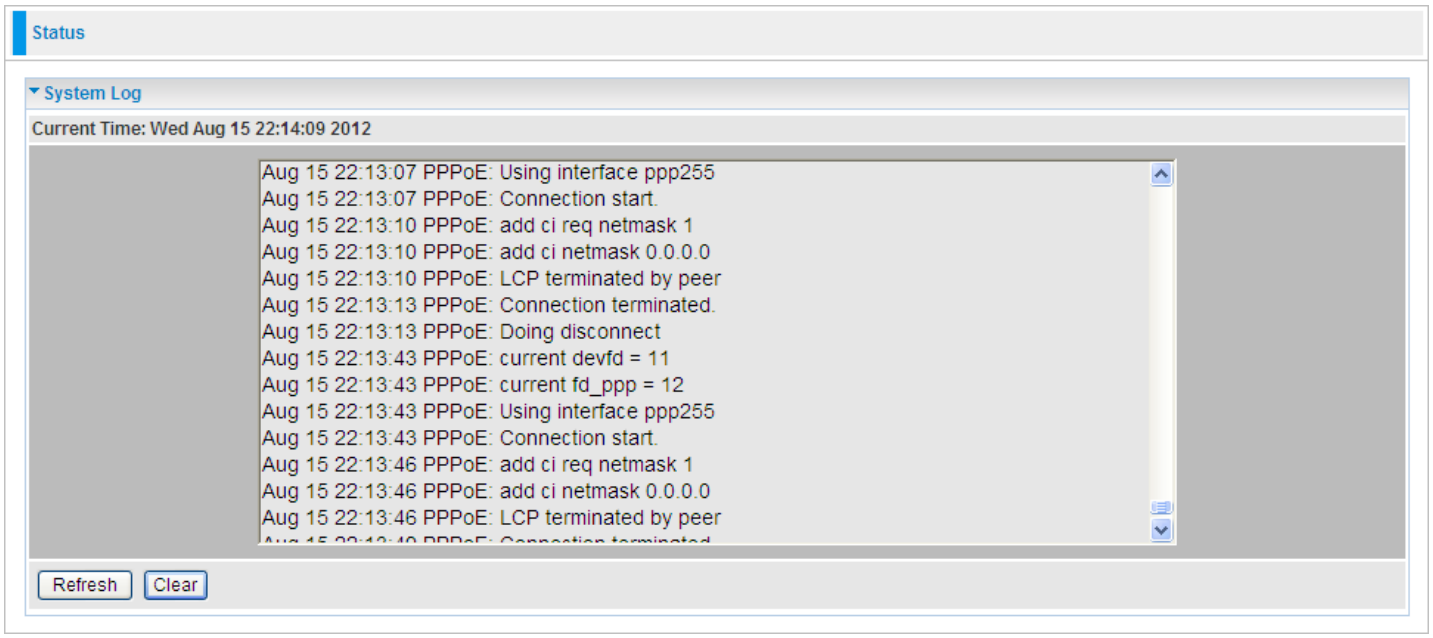
MAC Address: The MAC Address of internal DHCP client host.

Client Host Name: The Host Name of internal DHCP client.

Register Information: Register time information.

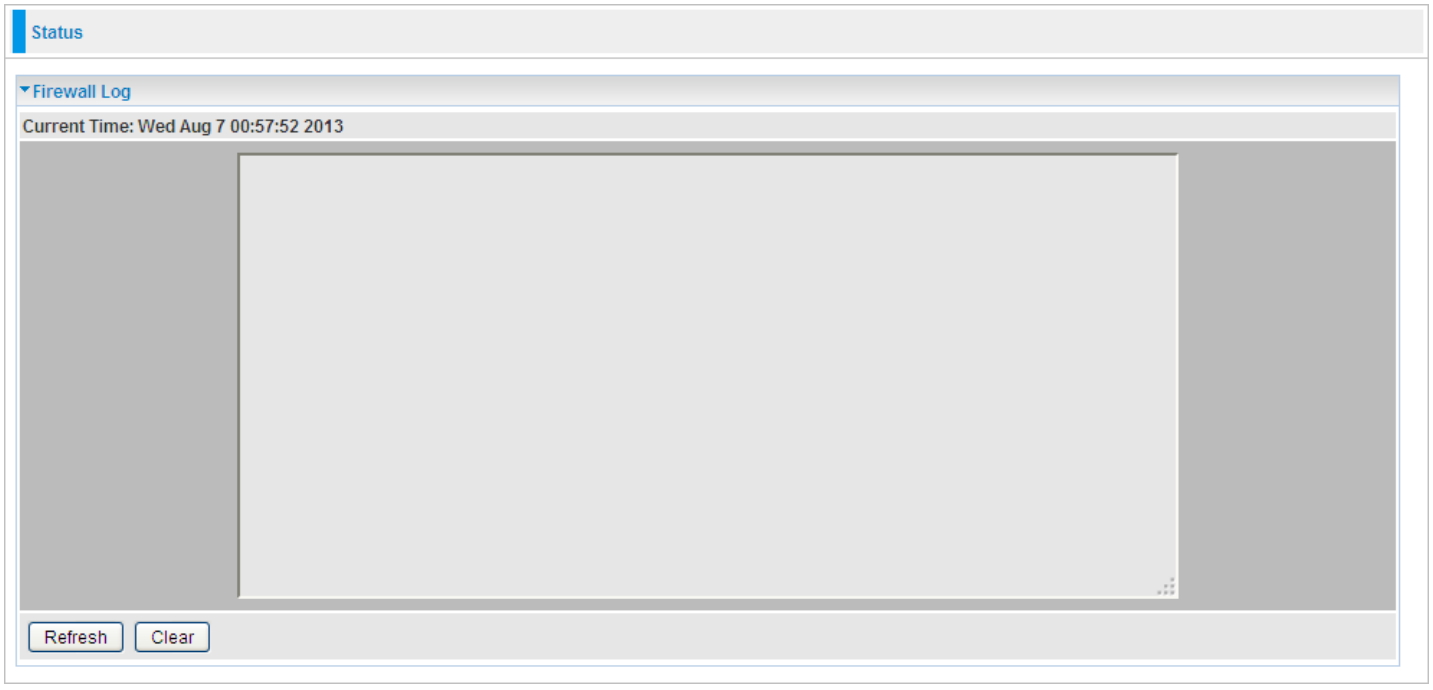
System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.


Status
System Log
Current Time: Wed Aug 15 22:14:09 2012
Aug 15 22:13:07 PPPoE: Using interface ppp255
Aug 15 22:13:07 PPPoE: Connection start.
Aug 15 22:13:10 PPPoE: add ci req netmask 1
Aug 15 22:13:10 PPPoE: add ci netmask 0.0.0.0
Aug 15 22:13:10 PPPoE: LCP terminated by peer
Aug 15 22:13:13 PPPoE: Connection terminated.
Aug 15 22:13:13 PPPoE: Doing disconnect
Aug 15 22:13:43 PPPoE: current devfd = 11
Aug 15 22:13:43 PPPoE: current fd_ppp = 12
Aug 15 22:13:43 PPPoE: Using interface ppp255
Aug 15 22:13:43 PPPoE: Connection start.
Aug 15 22:13:46 PPPoE: add ci req netmask 1
Aug 15 22:13:46 PPPoE: add ci netmask 0.0.0.0
Aug 15 22:13:46 PPPoE: LCP terminated by peer
Refresh
Clear

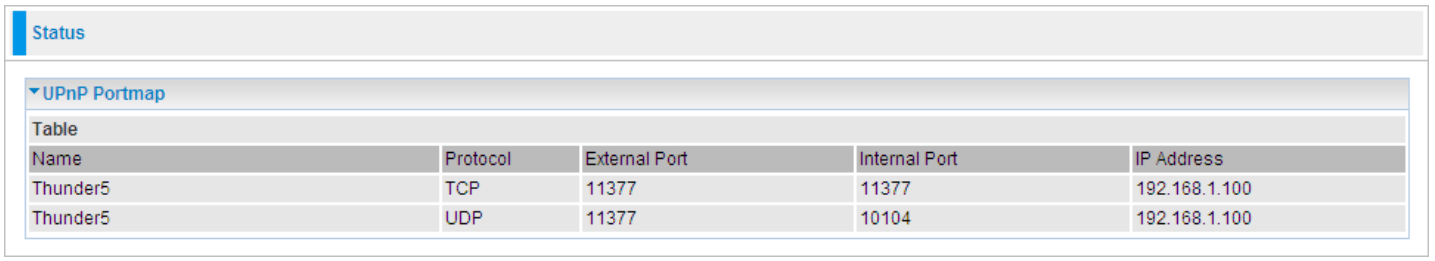
Firewall Log

Firewall Log displays log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration / Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced Configuration section of this manual for more details on UPnP and the router's UPnP configuration options.



Name: the name of this UPnP mapping.

Protocol: the protocol used by this mapping.

External Port: the external service port the internal port mapped to.

Internal Port: the internal service port.

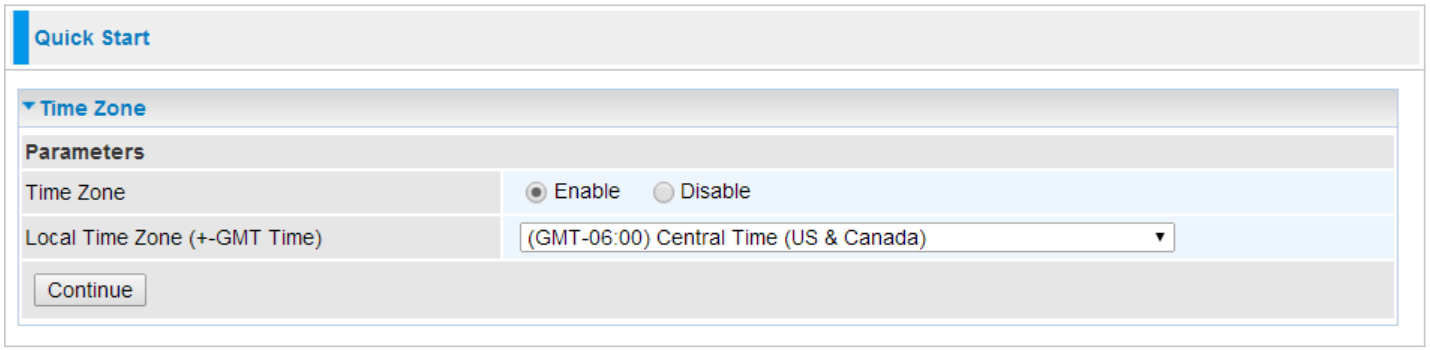
IP Address: the IP Address of the host in LAN.

Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup time zone and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

Step 1 – Time Zone

Enable and Select the appropriate Time Zone, then click **Continue** to go on to next step. You can turn **Time Zone** to understand more.

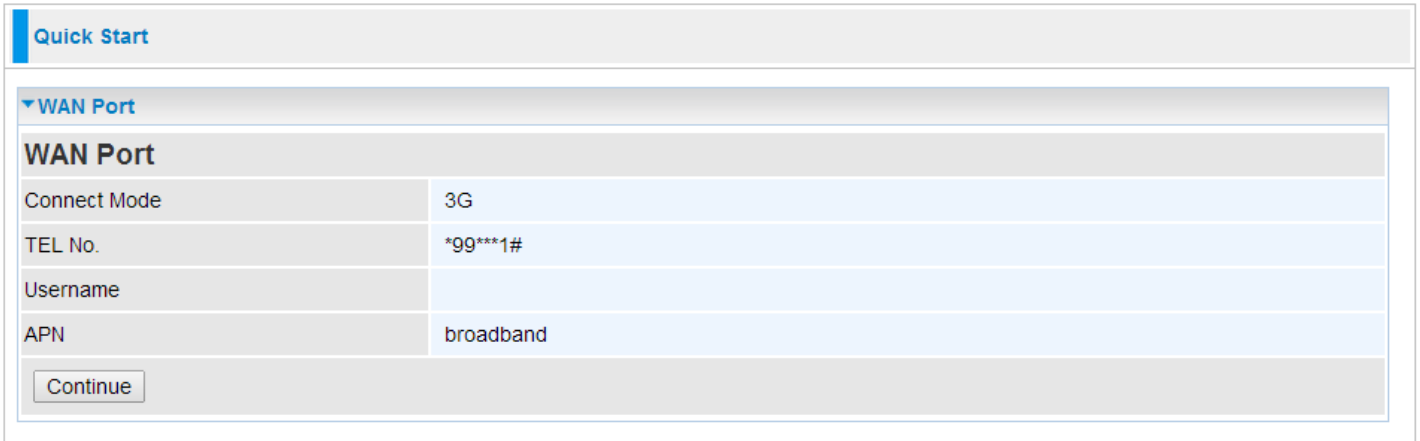


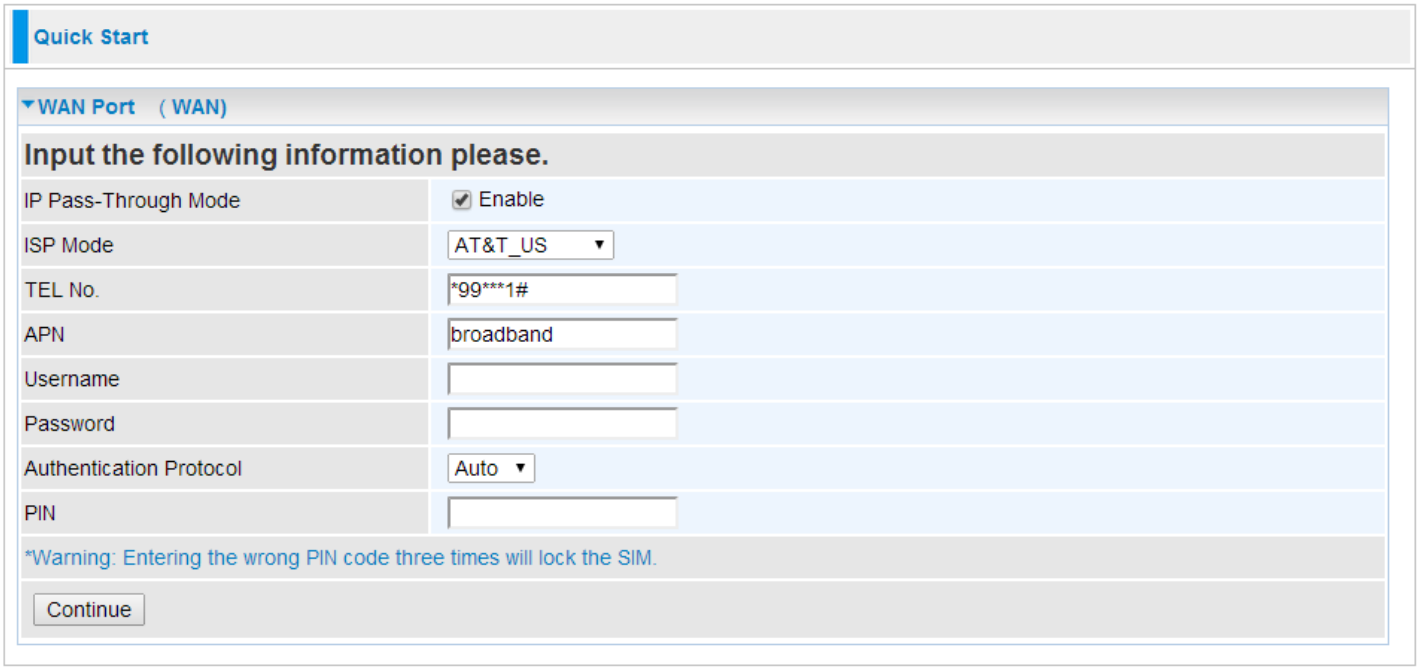
Step 2 – WAN

Click **Continue** to enter your SIM card inform for registration.

Enter your SIM card telephone number, APN, Username, Password, PIN, etc.

If you have trouble to find these information, please consult with your SIM carrier.





Note: when re-inserting the 3G / 4G SIM card to the BEC 6800RUL, you should again press Continue button to make 3G / 4G connection take effort, or you can Save Config and Restart the router to reach the same effort.

Step 3 – Configuration in Process

The 6800RUL will take 15~30 seconds to configure the settings. Once it is done, you will see a "Configurations!" window.

Step 4 – Quick Start Completed!

You now may be able to access to the Internet. If not, please check your WAN, Internet Connection, setup again.

To review the WAN connection, please go back to **Status** for more information.

Configuration

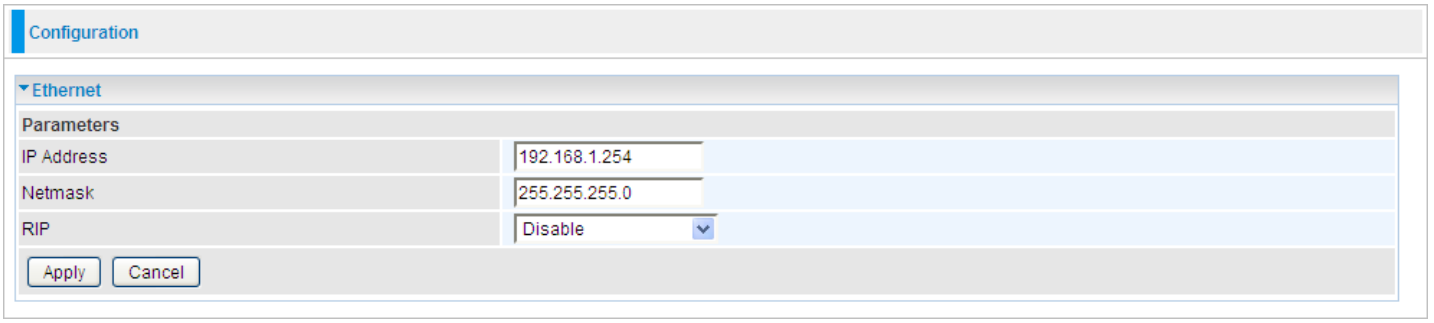
Click this item to access the following sub-items that configure the 3G / 4G router: **LAN, WAN, System, Firewall, QoS, Virtual Server, Time Schedule,** and **Advanced.**

These functions are described in the following sections.

LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

Ethernet



The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

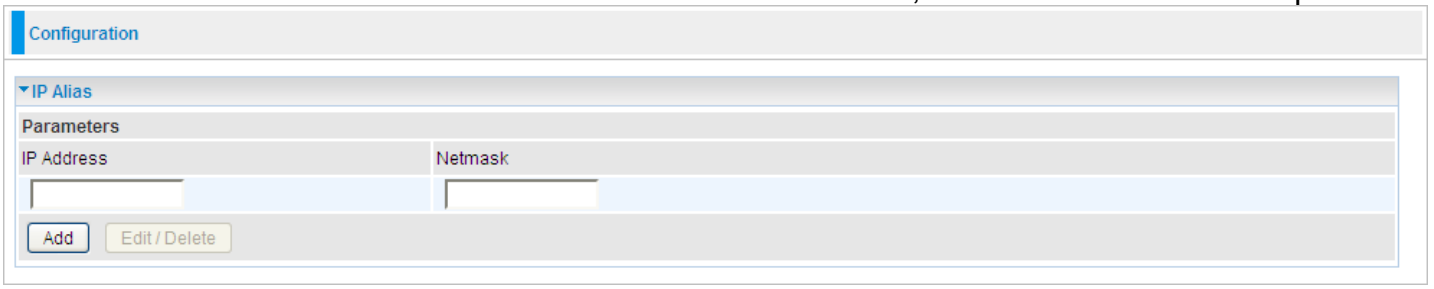
IP Address: The IP on this router, default is 192.168.1.254.

Netmask: The subnet mask on this router.

RIP: RIP v1, RIP v2 Broadcast, RIP v1+v2 Broadcast and RIP v2 Multicast.

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



IP Address: Specify an IP address on this virtual interface.

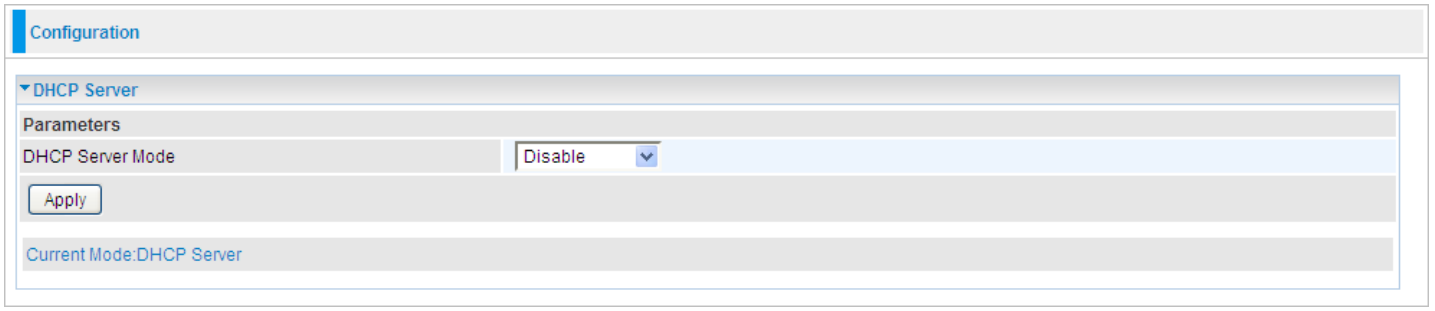
Netmask: Specify a subnet mask on this virtual interface.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

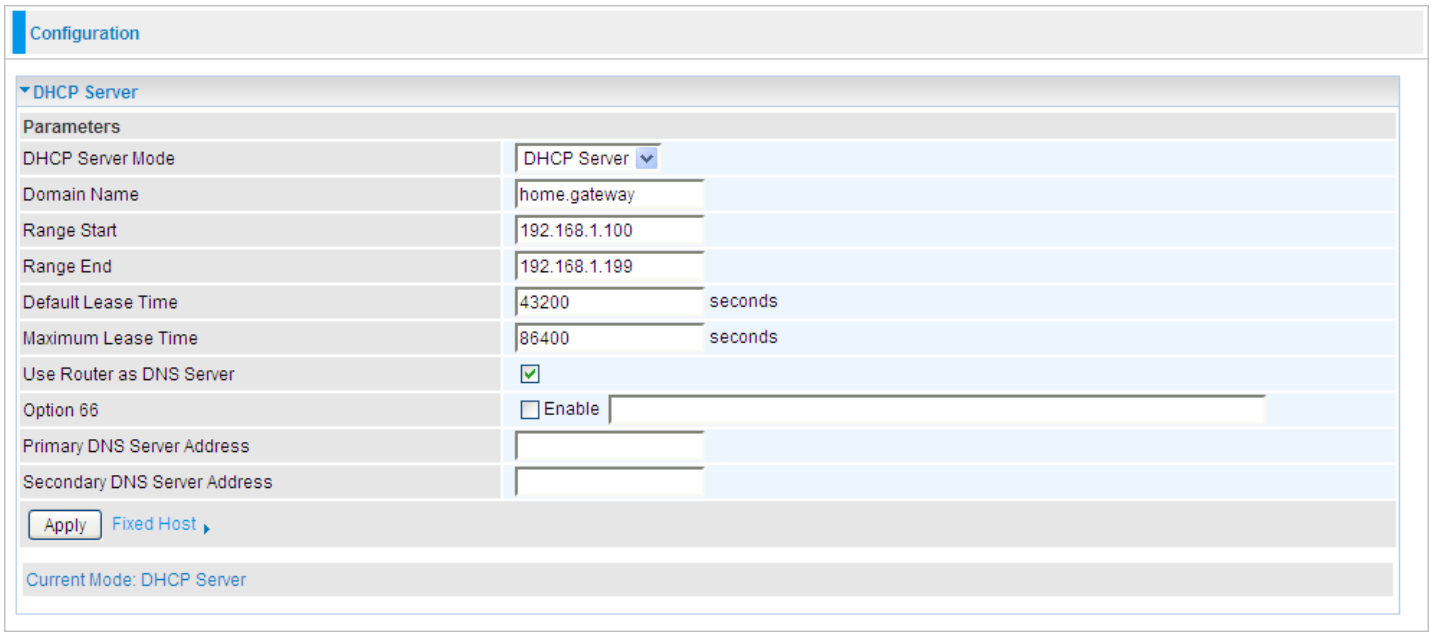
DHCP Server Mode: Disable

To disable the router's DHCP Server, check **Disabled** and then click **Apply.** When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).



DHCP Server Mode: DHCP Server

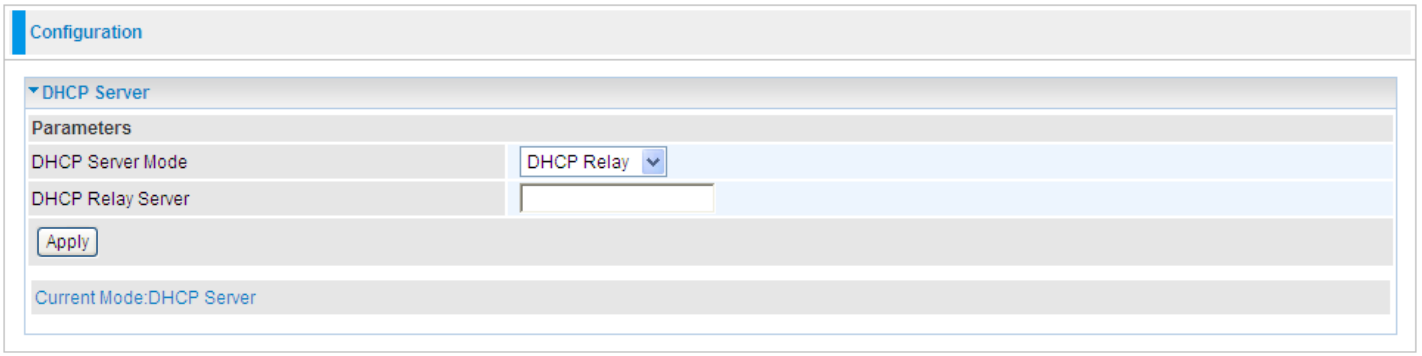
To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the 3G / 4G Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).



DHCP option 66: This option is used to identify a TFTP server for convenient configuration downloading for clients. **Enable** to use option 66 and be sure to enter the TFTP server IP or domain name information.

DHCP Server Mode: DHCP Relay

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.

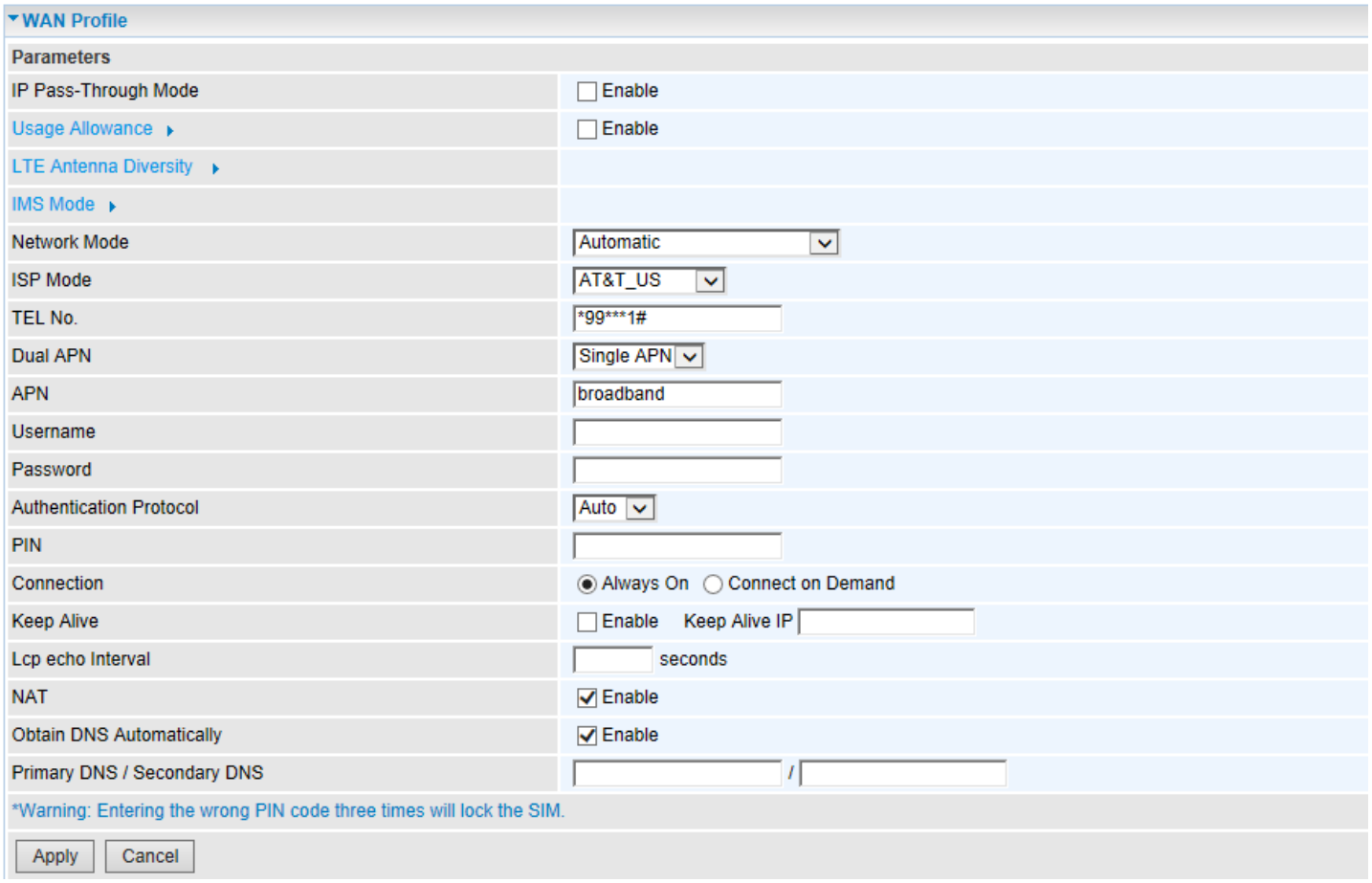


WAN - Wide Area Network

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

WAN Profile

Prior to configuring this WAN profile for your SIM card, please first inserting a 3G/4G_LTE SIM Card into to the built-in SIM slot in the BEC 6800RUL.



IP Pass-through Mode: When **enabled**, BEC 6800RUL is in bridge mode that it does not obtain a WAN IP address; features such as routing capabilities, NAT, firewall, etc., are being disabled. The client router that is behind the BEC 6800RUL now obtains a WAN IP address. When **disabled**, BEC 6800RUL is in router mode that it handles a WAN IP address and all features become available.

Usage Allowance: When **enabled**, you can control and manage your mobile usage. Please click here for detailed setup instruction.

LTE Antenna Diversity: When **enabled**, the auxiliary antenna will be activated. With **disabled**, only the primary antenna is receiving and transmitting data.

NOTE: When using Yagi antenna, please DISABLE the Antenna Diversity feature for utmost performance.

IMS Mode: (for Mobile Service Provider used only)

Network Mode: If you know the appropriate Network mode you need to connect to, please select it from the list; otherwise, select “Automatic.

ISP Mode: A list of 3G / 4G service providers that is available.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by

your mobile service provider.

Dual APN: Our 3G/4G router provides your either Single APN (one WAN IP) or Dual APN (dual WAN IP) to meet users' different demands. Enter corresponding APN(s) from your service providers.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G / 4G operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Auth. Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

NOTE: If you enter an incorrect PIN code three times (3) in a row, your SIM card will be blocked. In this case, please enter your PUK code (it can be supplied by your service provider) and then re-enter your PIN.

Connection:

- **Always On:** The router will make UMTS/GPRS call when starting up. Enabling Always On, will give you an option of Keep Alive.
- **Connect to Demand:** When enabling this feature, the BEC 6800RUL will automatically resume its Internet connection when there is a packet requesting from a local LAN device.

Keep Alive: Click to enable keep alive mechanism. User should set the Keep Alive IP to necessitate the always on connection. The IP is used for ping operation to examine whether the connection is still on.

Lcp echo Interval: Set the interval time (seconds), if set to 5, that means the router is allowed to send message out every 5sec to prevent the connection being dropped by ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

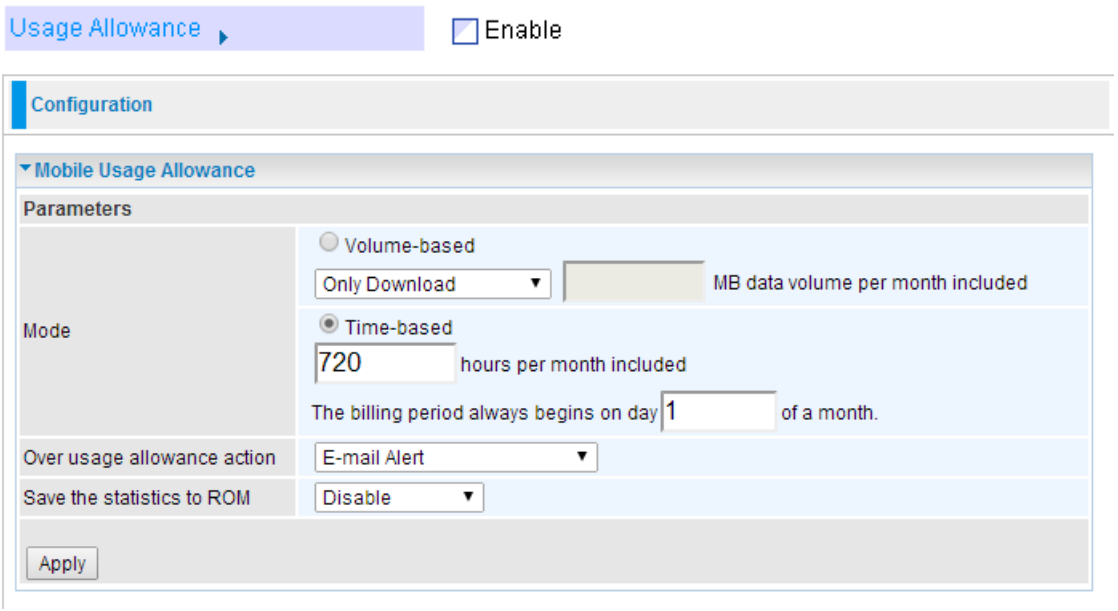
Obtain DNS Automatically: Select this checkbox to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

NOTE: If you are not familiar with these settings, please consult with ISP for further assistance or information.

NOTE: After inserting your 3G/4G SIM card, please wait for 30 seconds before the dial-up connection process. If errors occur, please remove your SIM card or restarting your BEC 6800RUL router.

WAN Profile / Mobile Usage Allowance – Detailed setup instruction

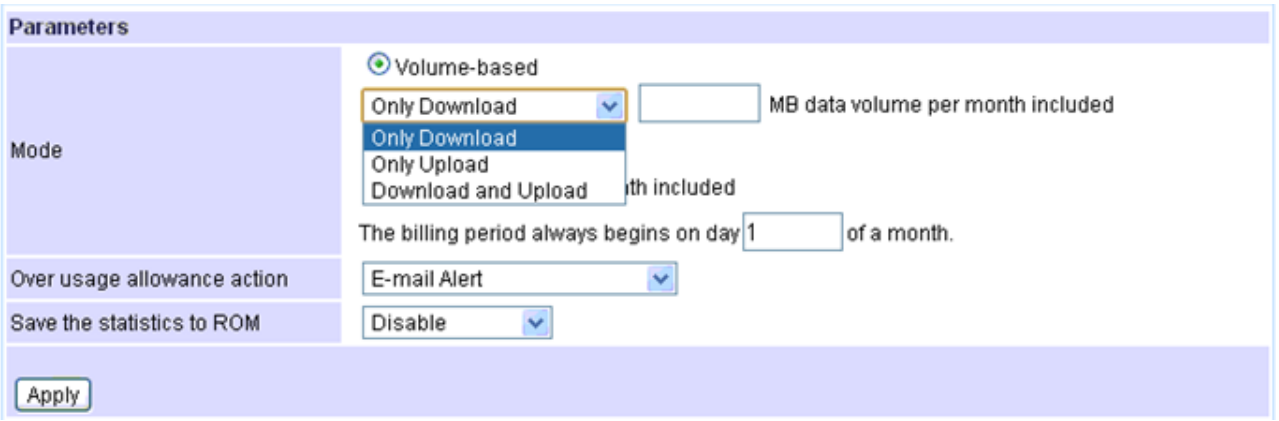


In order to query online time or volume used, you can set the following options.

Mode: Two methods are provided, that is, **Volume-based** and **Time-based**.

- **Volume-based:** If choosing **Volume-based**, you can view the volume you have used.
- **Time-based:** If choosing **Time-based**, you can view the online hours you have used.

Volume-based



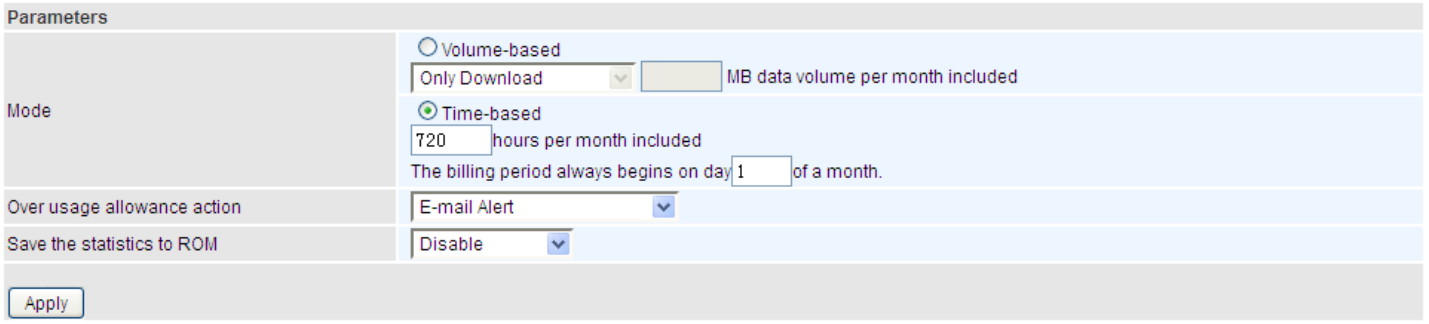
Only Download: Only make statistics of Download Traffic.

Only Upload: Only make statistics of Upload Traffic.

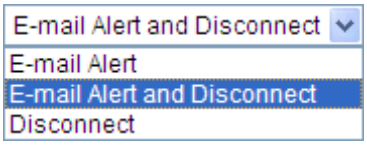
Download and Upload: Make statistics of both Download and Upload Traffic.

Time-based

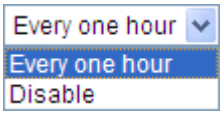
Allow you to manually assign a billing period.



Over usage allowance action: If the online time or traffic you have used exceeds the usage allowance you set. The system will do the followings operations.



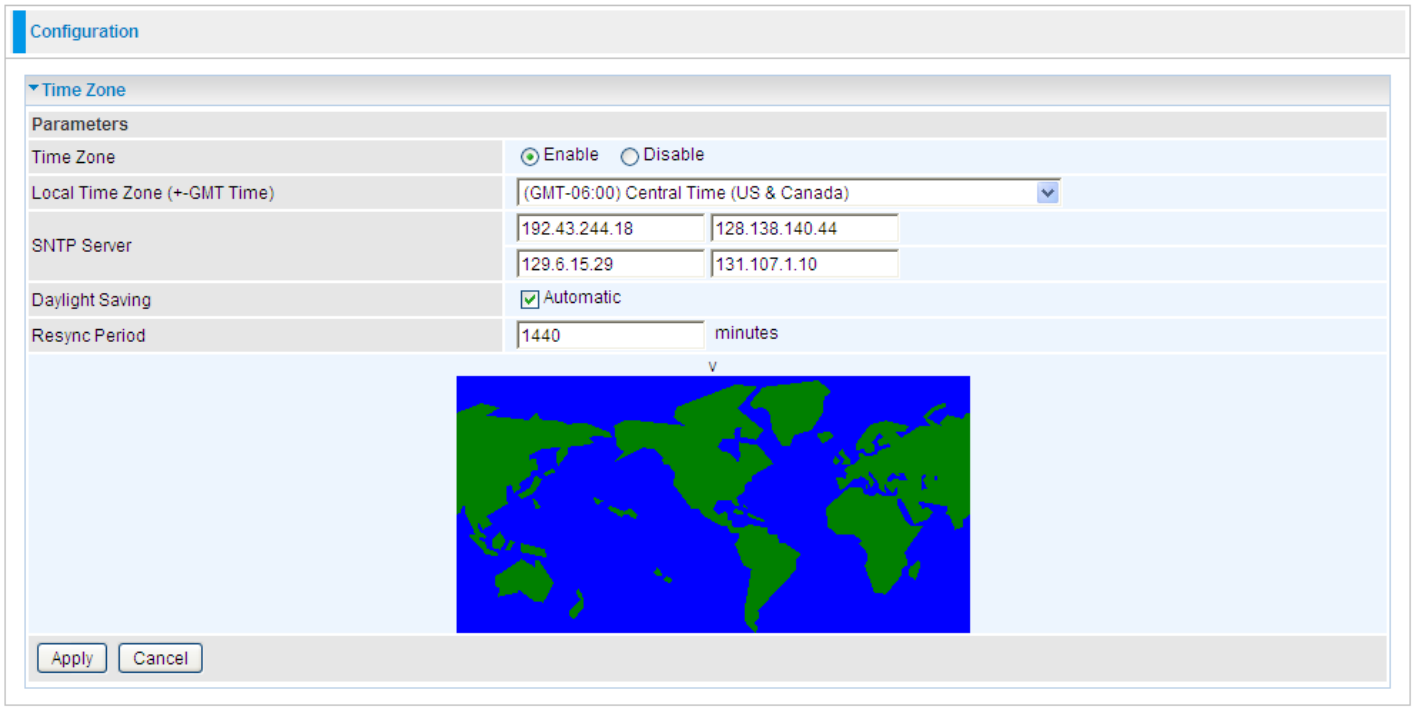
Save the statistics to ROM: Choose the time interval for saving statistics. You can choose to save for **Every one hour** or **Disable** the function**.**



System

The **System** section contains instruction for setting up local time zone, updating device system firmware, retrieving current device configuration for a copy or restoring a saved configuration file when accidently misconfigured the device, managing your login device information or setting up multiple account levels for others to access to this router, and send mail alert to inform you changes of your settings.

Time Zone



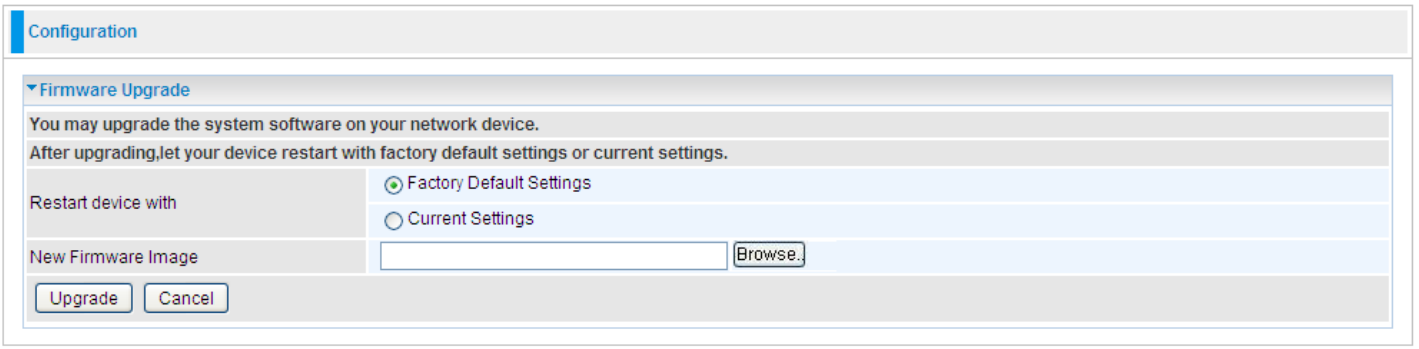
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



Restart Device with: To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).

New Firmware Image: Type in the location of the file you wish to upload in this field or click **Browse…** to locate it.

Browse…: Click **Browse…** to find the file with the **.afw** file extension that you wish to upload.

NOTE: You must uncompress / unzip the .zip file before you can upgrade the file.

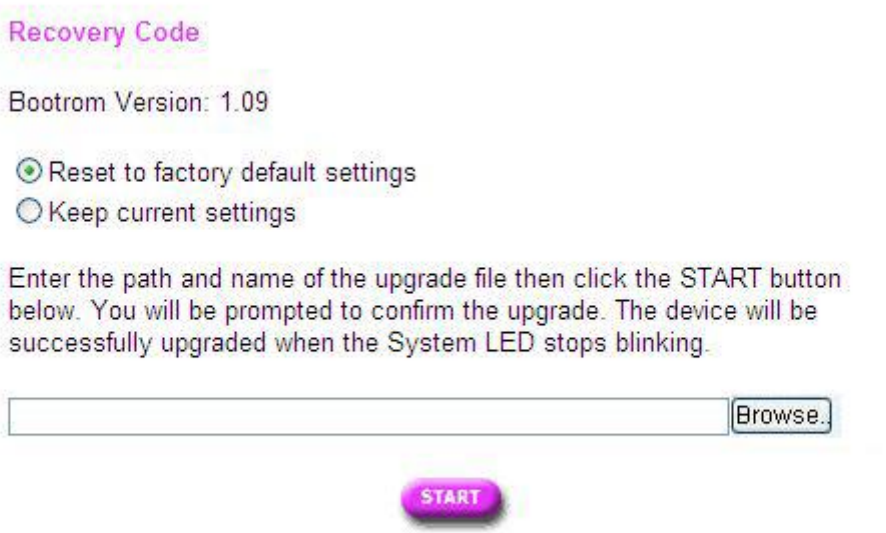
Upgrade: Click **upgrade** to begin the upload process. This process may take up to three minutes.

Warning

Do not power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. If firmware upgrade failure occurs, please refer to operations below for emergency recovery.

Recovery Procedure

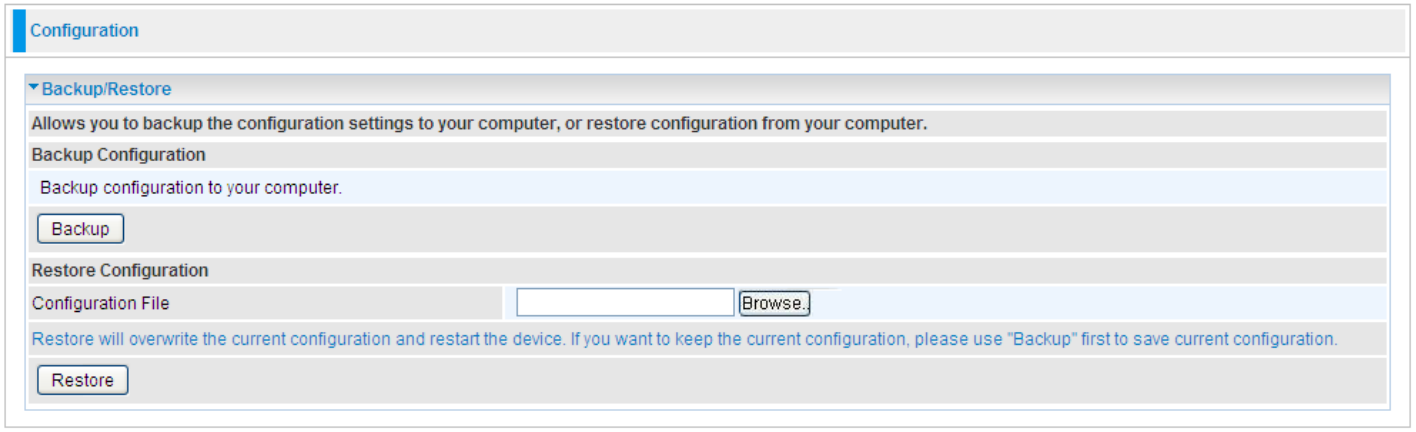
If your device's upgrade failed, then you can take emergency recovery procedure to recover. Usually, if the device failed to upgrade successfully, the recovery page will automatically (or you enter 192.168.1.254 at the address bar) turn to the page showed as below, entering the recovery mode.


Recovery Code
Bootrom Version: 1.09
Reset to factory default settings
Keep current settings
Enter the path and name of the upgrade file then click the START button below. You will be prompted to confirm the upgrade. The device will be successfully upgraded when the System LED stops blinking.
Browse...
START

Select the correct file used for upgrade, and press **START**.

Backup / Restore

It allows you to save and backup your router's current settings, in a readable format, on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. Highly recommended you backup your router's settings before and after any changes to your router.


Configuration
Backup/Restore
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse..
Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

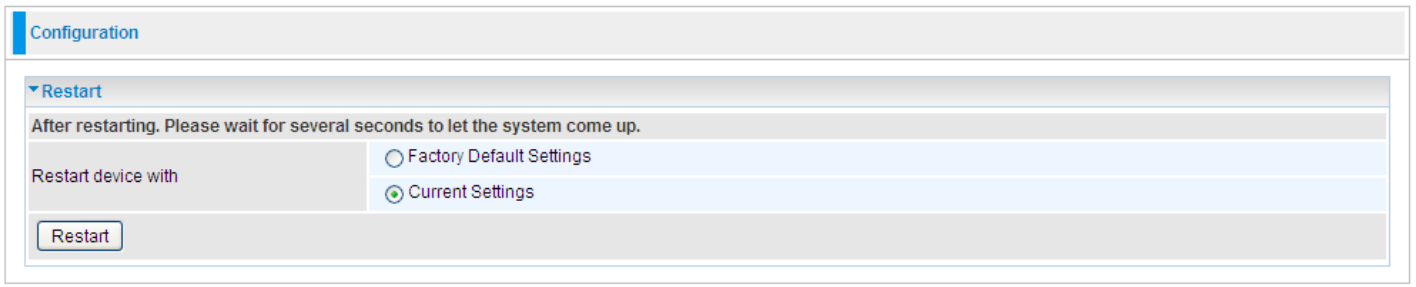
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse…** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

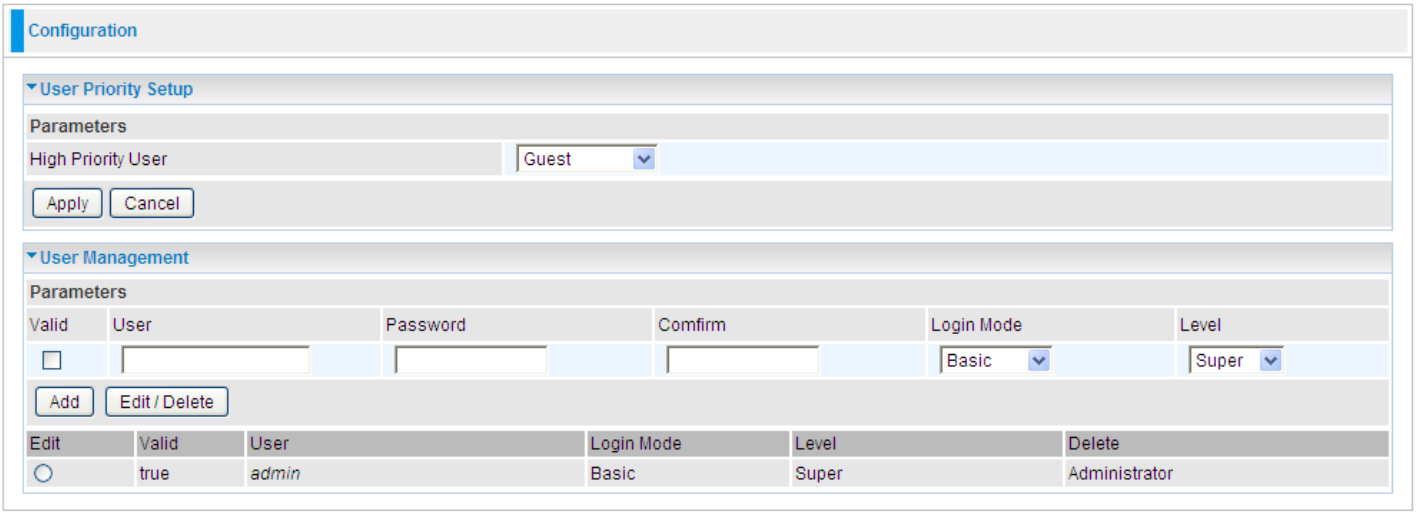
Restart Router

Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

User Management



In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

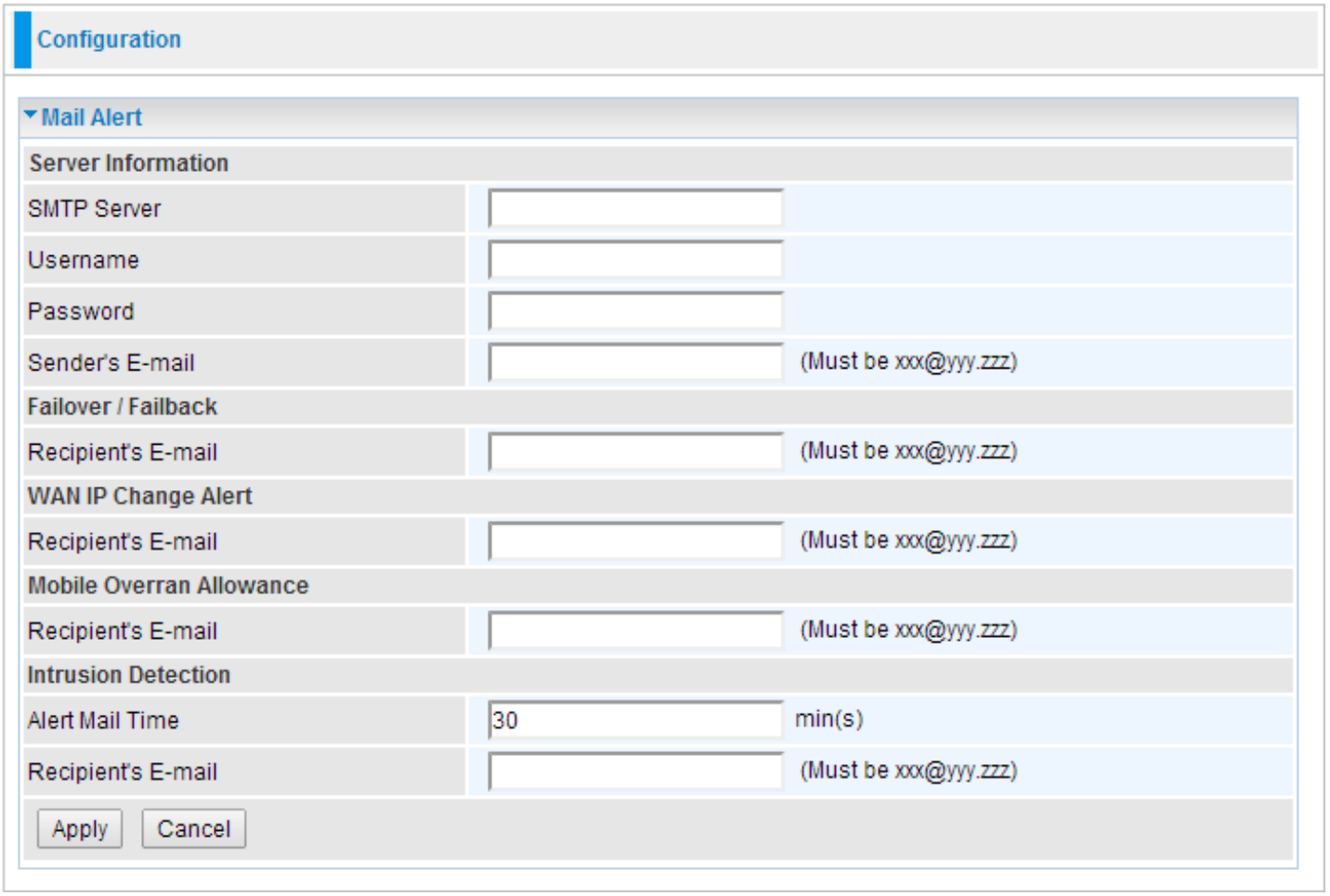
You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit**,** the information of the account will be displayed above. Just go ahead and change the password.

You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.

It is highly recommended to change your router password to something unique that only you know it when you receive this unit. If at any time you forget this password, please press and hold the RESET button in the rear panel for more than 6 seconds then release it for router to restore to its factory default settings.

Mail Alert

Mail Alert is designed to keep you as the router administrator or other relevant personnel alerted of any change to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

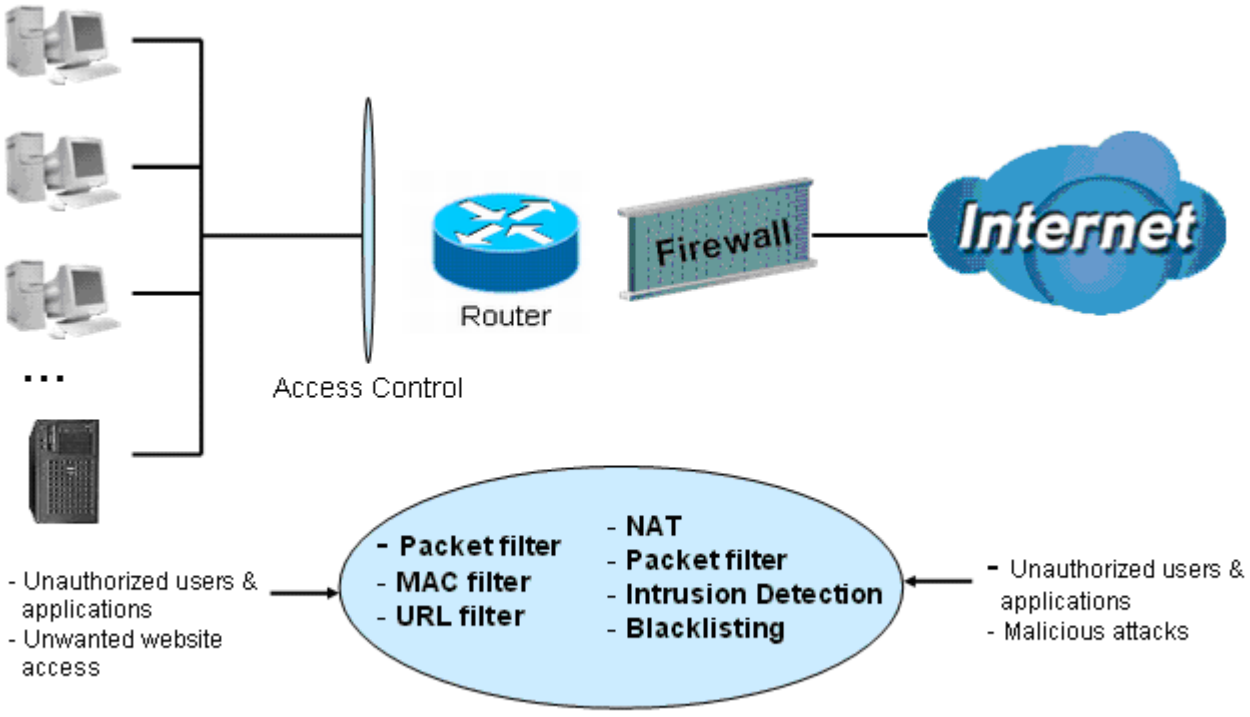
Recipient's Email (Mobile Overran Allowance): Enter the email address that will receive the alert message once 3G / 4G overran allowance was detected.

Alert Mail Time (Intrusion Detection): The time interval of sending Email.

Recipient's Email (Intrusion Detection): Enter the email address that will receive the alert message once intrusion has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall & Filter

Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users’ IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

NOTE: When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

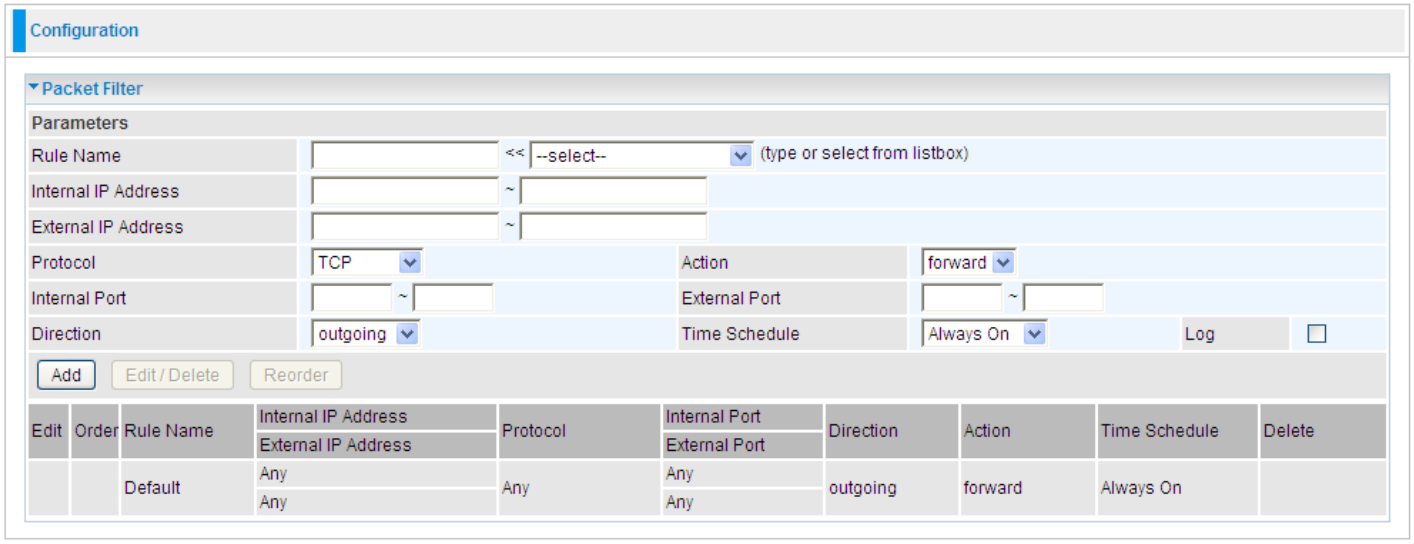
Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

URL Filter: Blocks PCs on your local network from unwanted websites.

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Rule Name: Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from list box.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/from particular IP addresses. Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to.

Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

Action: If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535.** It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Log: Choose "log" if you wish to generate logs when the filer rule is applied to a packet.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check the Rule No. you wish to edit, and then click "Edit".

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

Edit	Order	Rule Name	Internal IP Address External IP Address	Protocol	Internal Port External Port	Direction	Action	Time Schedule	Delete
○	↓	FTP	Any Any	TCP	Any 21~21	outgoing	forward	Always On	☐
○	↑	TELNET	Any Any	TCP	Any 23~23	outgoing	forward	Always On	☐
		Default	Any Any	Any	Any Any	outgoing	forward	Always On	

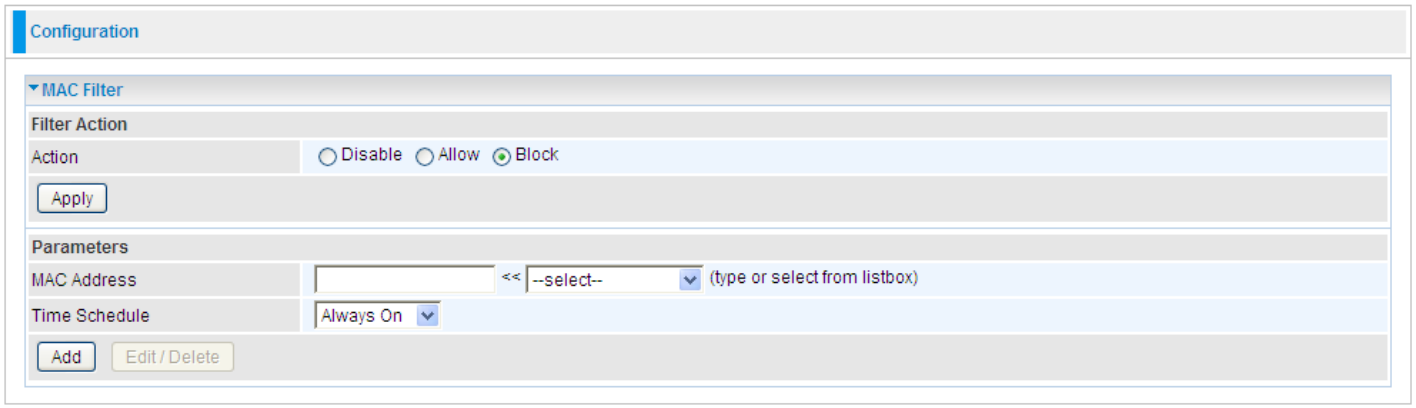
Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.



Action： select to determine how to do with the filter.

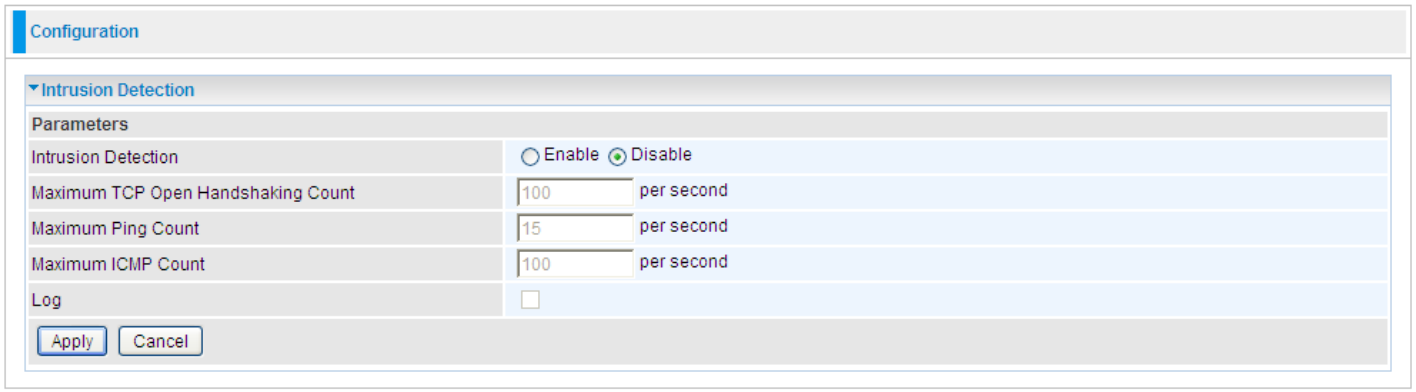
- **Disable:** to disable the MAC filter function.
- **Allow:** to enable the MAC filter function and allow the host of the following set MAC addresses to access.
- **Block:** to enable the MAC filter function and block the host of the following set MAC addresses to access.

MAC Address: Enter the MAC addresses you wish to manage.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.



Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Maximum Ping Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Maximum ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Check Log if you wish to generate logs when the filer rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.

Hacker attack types recognized by the IDS

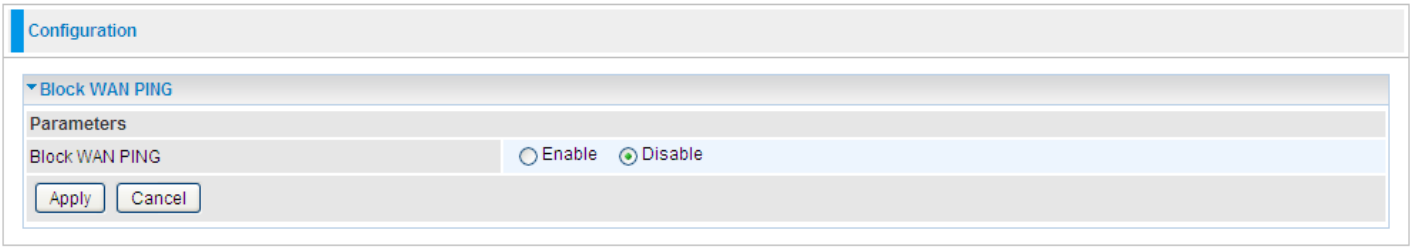
Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP **Src Port:** Source Port

Dst Port: Destination Port **Dst IP:** Destination IP

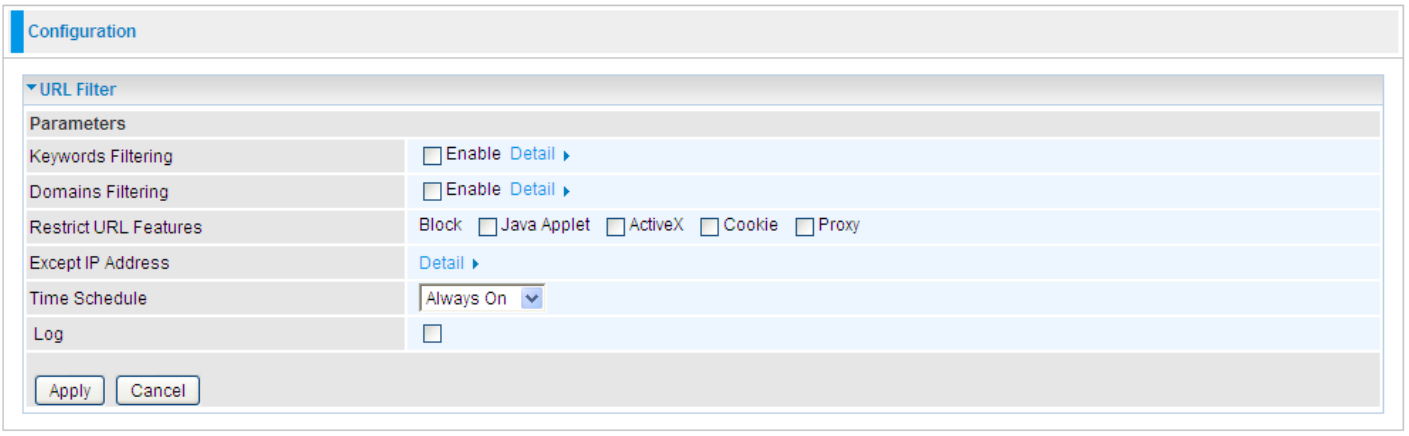
Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.



URL Filter

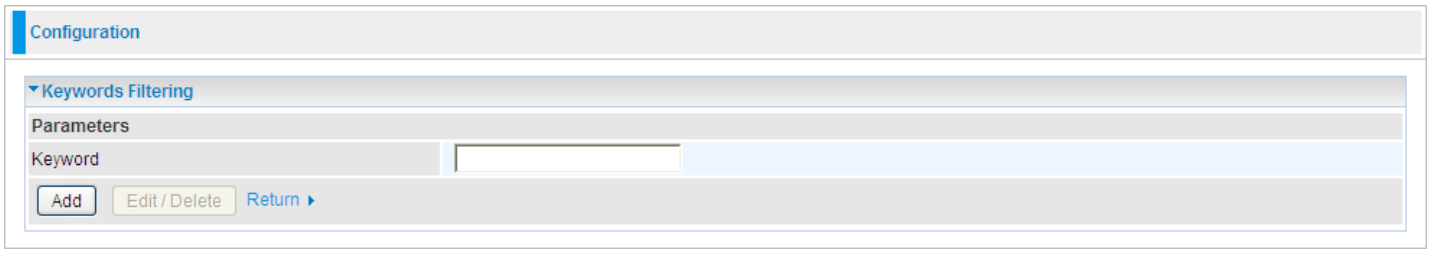
URL (Uniform Resource Locator – e.g. an address in the form of **http://www.example.com**) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Keywords Filtering

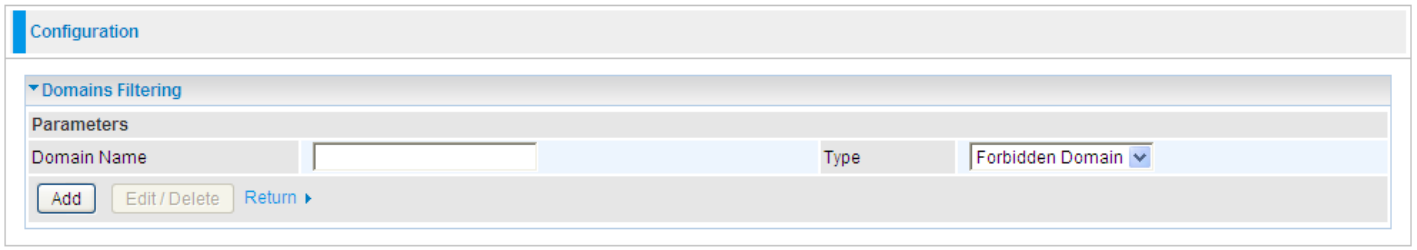
Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL http://www.abc.com/abcde.html would be dropped since the keyword “abcde” occurs in the URL.



Domain Filtering

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”



Restrict URL Features

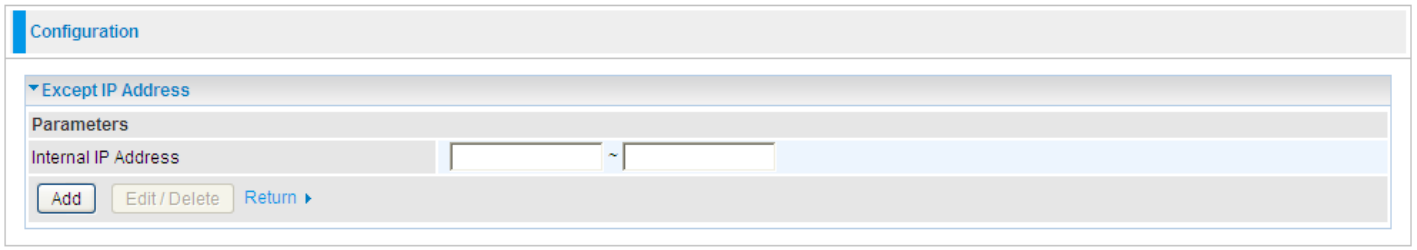
The router will automatically filter out the selected features.

- **Block Java Applet:** Blocks Java Applet
- **Block ActiveX:** Blocks ActiveX
- **Block Cookies:** Blocks Cookies
- **Block Proxy:** Blocks Proxy

Except IP Address

Once enabled, the URL filtering will apply to all devices that are associating with the router.

If you wish to be excluded from the filtering group, please enter your device’s IP or an IP range.



Time Schedule

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log

Log: Click “Log” if you wish to generate logs when the filer rule is applied to the URL Filter.

QoS - Quality of Service

Quality of Service Introduction

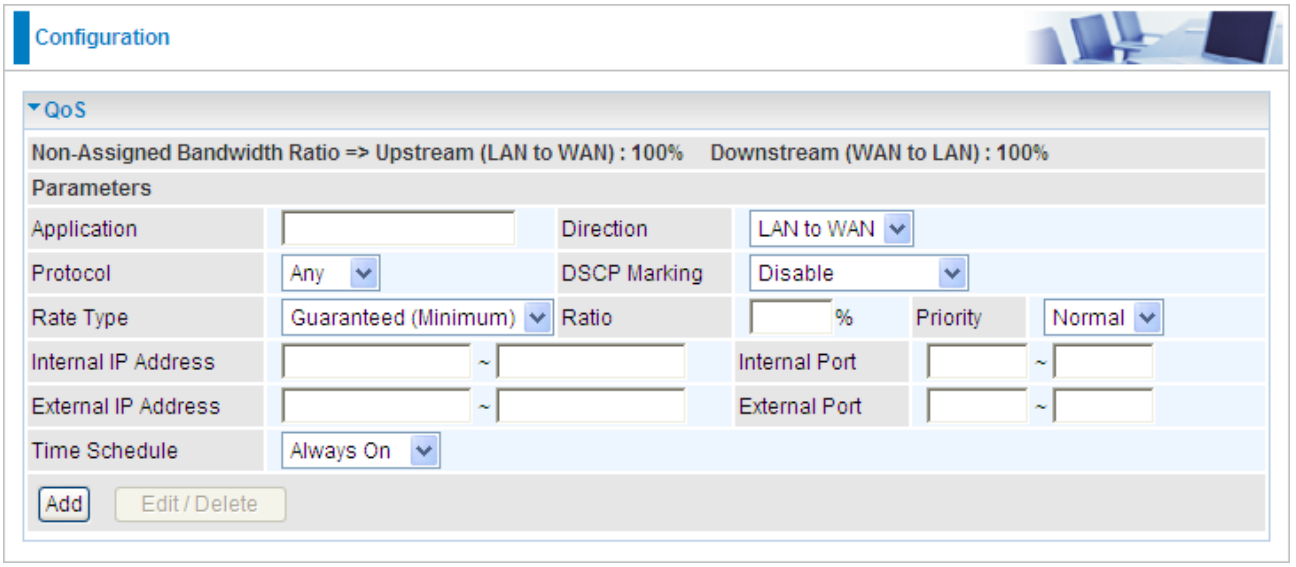
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.



After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: A name that identifies an existing policy.

Direction: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

- **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.
- **WAN to LAN**: Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

- **ANY:** No protocol type is specified.
- **TCP**
- **UDP**
- **ICMP**
- **GRE**

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

NOTE: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

The DSCP Mapping Table

DSCP Mapping Table	
3G / 4G Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: 2 types are provided:

- **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- **Guaranteed (Minimum):** Specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

Priority: Specify the priority for the bandwidth that is not used. For examples, you may specify two different QoS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

- **High**
- **Normal**: The default is normal priority.
- **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

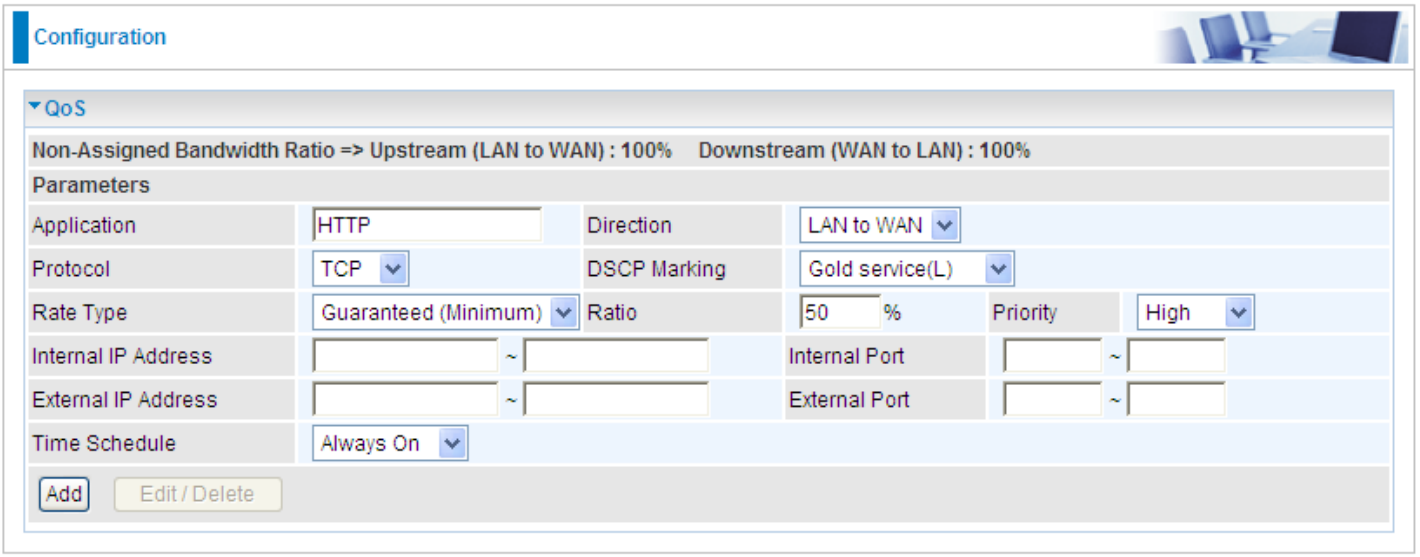
Example: QoS for your Network

If you are actively engaged in using P2P and are afraid of slowing down internet access throughput of other users within your network, you can thus use QoS function to set different priorities and bandwidth ratio for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

The figures below are a simple example to show the different settings for Web Browsing and Email sending to assure the bandwidth for these applications.

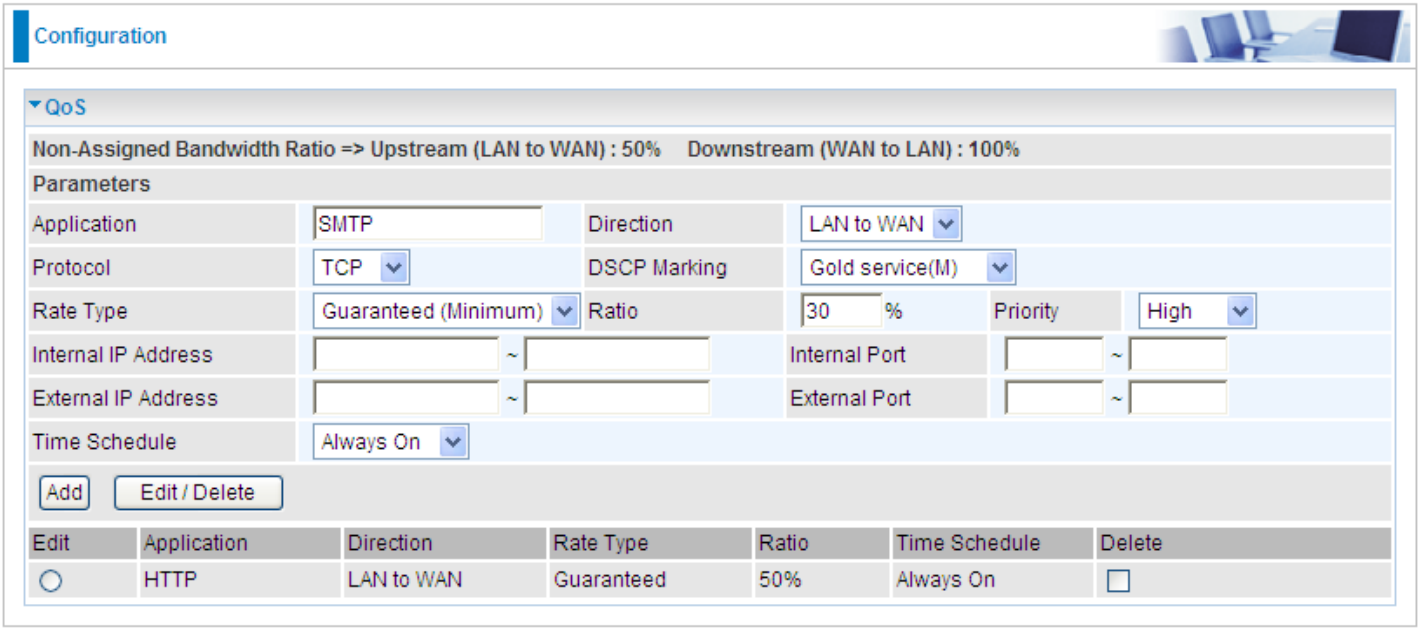
For Web Browsing (HTTP)

Here we guarantee 50% of the traffic for HTTP application.



For Mail Sending (SMTP)

Here we guarantee 30% of the traffic for Mail application.



Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
○	HTTP	LAN to WAN	Guaranteed	50%	Always On	☐
○	SMTP	LAN to WAN	Guaranteed	30%	Always On	☐

Thus, 20% of LAN to WAN (upstream) traffic is reserved for other uses and those applications' bandwidths are guaranteed.

For downstream traffic bandwidth, just the direction changes and the configuration is similar.

Virtual Server

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

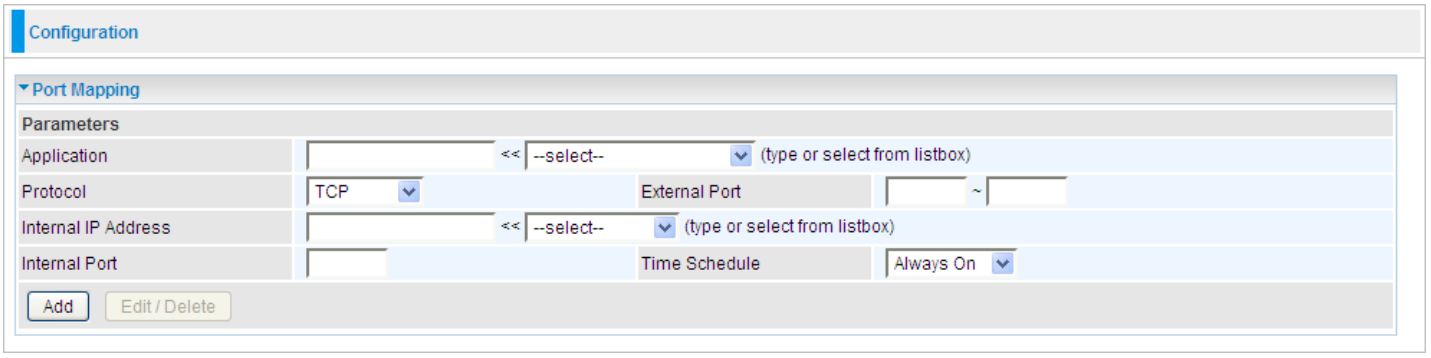
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Port Mapping



Application: Select the service you wish to configure.

Protocol: Automatic when you choose Application from list-box or select a protocol type which you want.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

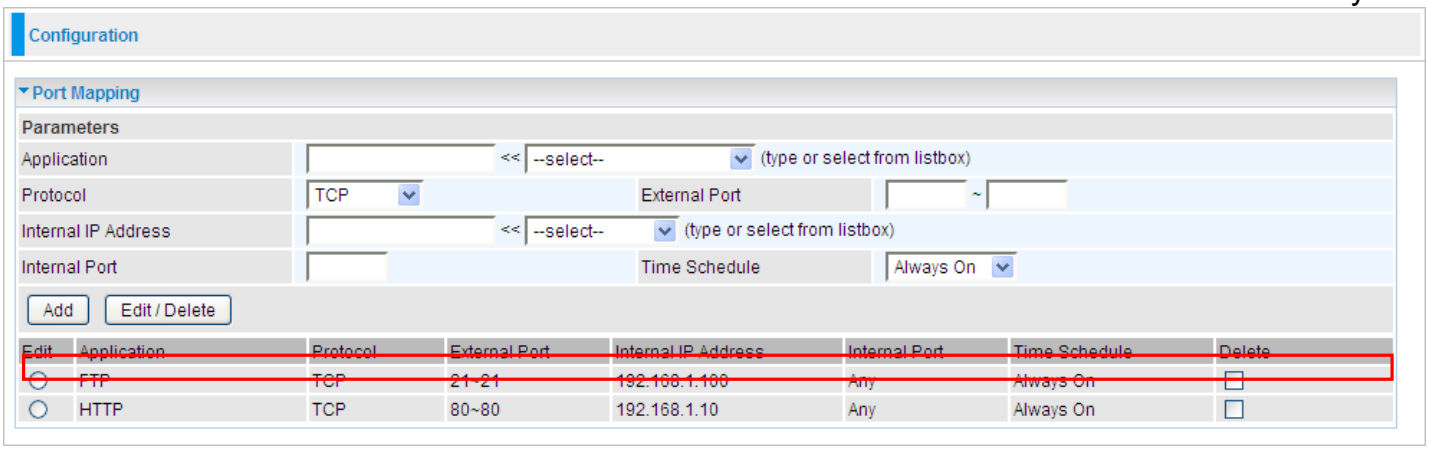
Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Rule No. you wish to edit and then click “Edit/Delete”.

Delete: Check the Rule No. you wish to delete then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

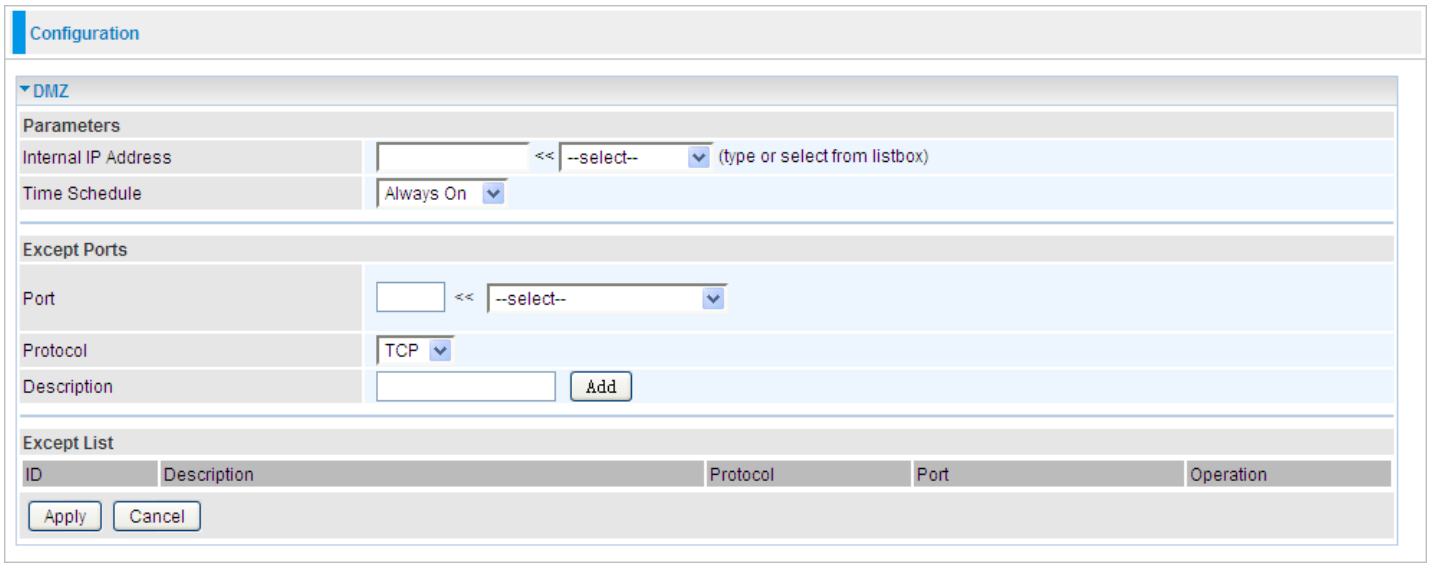


In addition to specifying the port number used, you also need to specify the protocol used. The

protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.



Internal IP Address: Enter the IP address of a specific internal server to which will be the DMZ Host.

Time Schedule: A self-defined time period. You may specify a time schedule. For setup and detail, refer to Time Schedule section.

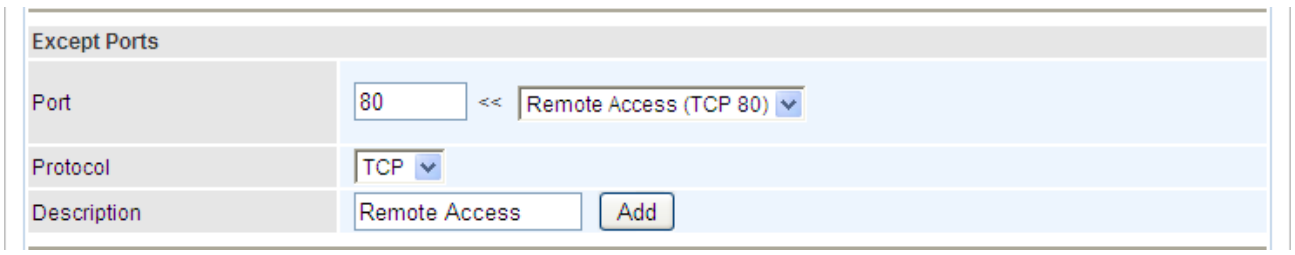
Port: The except port number. Default is set from range 1 ~ 65535.You can select from the drop down list and also can enter manually.

Protocol: Select the TCP or UDP protocol from the drop down list.

Description: The description of the port's function.

Add/Delete Except Ports

1. Enter except port number in the port field or choose from the drop down list. Select the port and describe the port.



2. Click **Add**. The new except port will display below.

Except List

ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete

Apply Cancel

3. Click **Delete** to delete the one which you want to remove from the Except List.

Except List

ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete
2	Printer Server	tcp	631	Delete
3	Web Cam	tcp	8081	Delete

Apply Cancel

NOTE:

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for "All" protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is disabled, you have to be very careful in assigning the IP addresses of the valid servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP addresses to each virtual server PC, with an address that does not fall into the range of IP address that are issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Configuration
Time Schedule
Parameters
Name
Day in a week
Sun Mon Tue Wed Thu Fri Sat
Start Time
08 : 00
End Time
18 : 00
Edit / Clear
Edit
Name
Day in a week
Start Time
End Time
Clear
TimeSlot1 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot2 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot3 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot4 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot5 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot6 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot7 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot8 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot9 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot10 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot11 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot12 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot13 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot14 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot15 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00
TimeSlot16 Sun Mon Tue Wed Thu Fri Sat 08:00 18:00

Name: A user-define description to identify this time portfolio.

Day in a week: The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

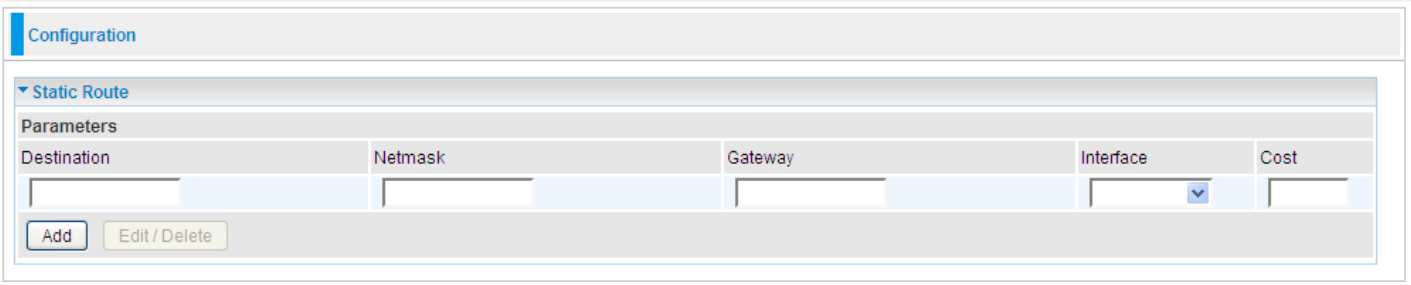
Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the Apply button to apply your changes.

Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Static Route



Destination: The destination subnet IP address.

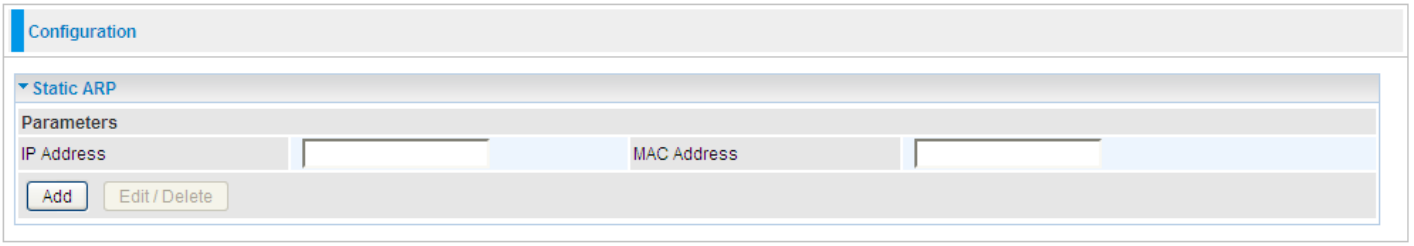
Netmask: Subnet mask of the destination IP addresses based on above destination.

Gateway: The gateway IP address to which packets are forwarded.

Interface: Select the interface through which packets are forwarded.

Cost: Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

Static ARP



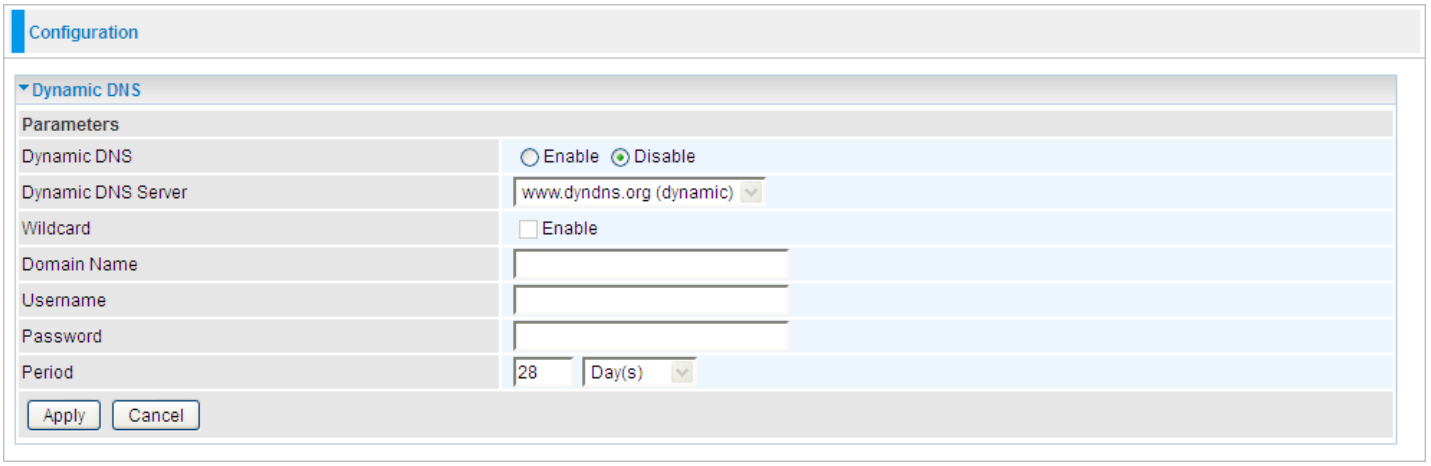
IP Address: Fill in the IP address of the host computer that is sending the data packet.

MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your 3G / 4G connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/.



Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The fields following are activated and required.

Dynamic DNS Server: Select the DDNS service you have established an account with.

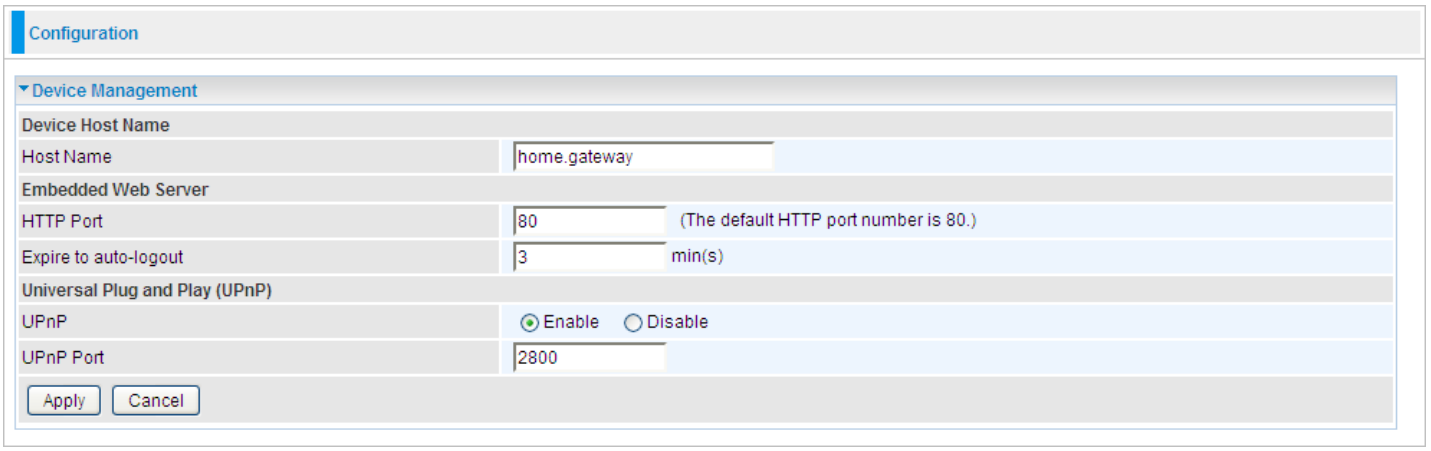
Wildcard: Select this check box to enable the DYNDNS Wildcard.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Embedded Web Server

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses. The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: **http://192.168.1.254:100** in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

UPnP Port: The Default setting is 2800. It is highly recommended you use this port value.

If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

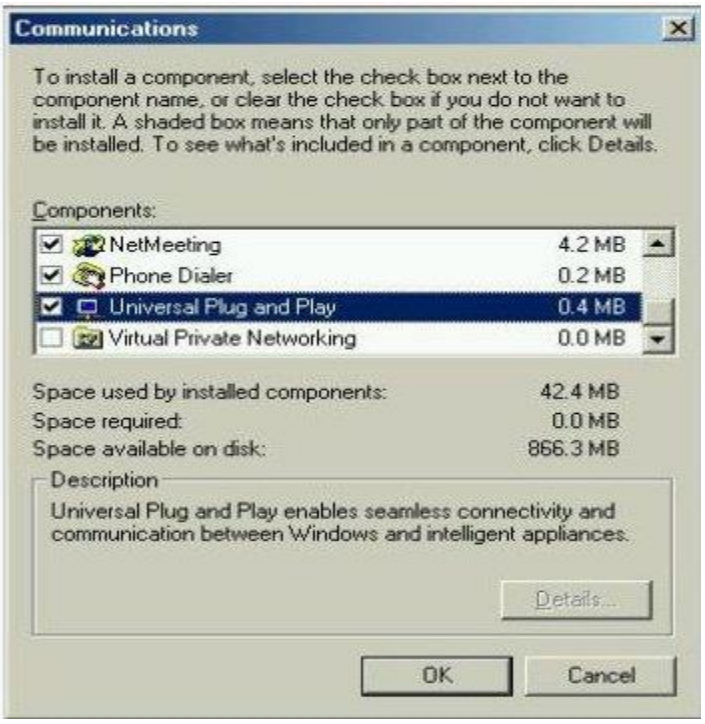
Follow the steps below to install the UPnP in Windows ME.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessibility 0.0 MB
Accessories 13.8 MB
Address Book 1.5 MB
Communications 7.0 MB
Desktop Themes 5.9 MB
Space used by installed components: 42.8 MB
Space required: 0.0 MB
Space available on disk: 2574.4 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 9 components selected
Details...
Have Disk...
OK
Cancel
Apply

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

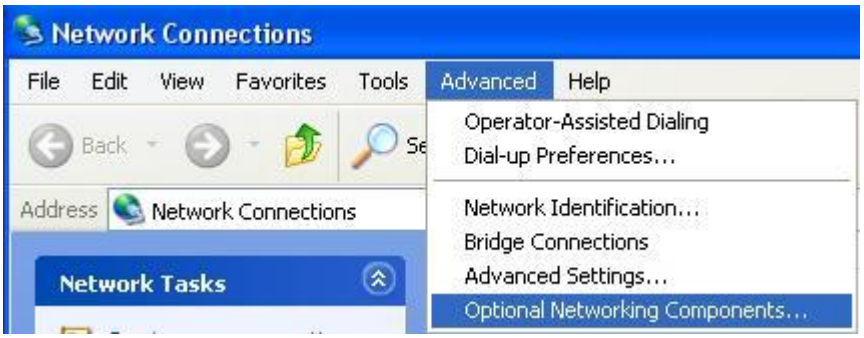
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

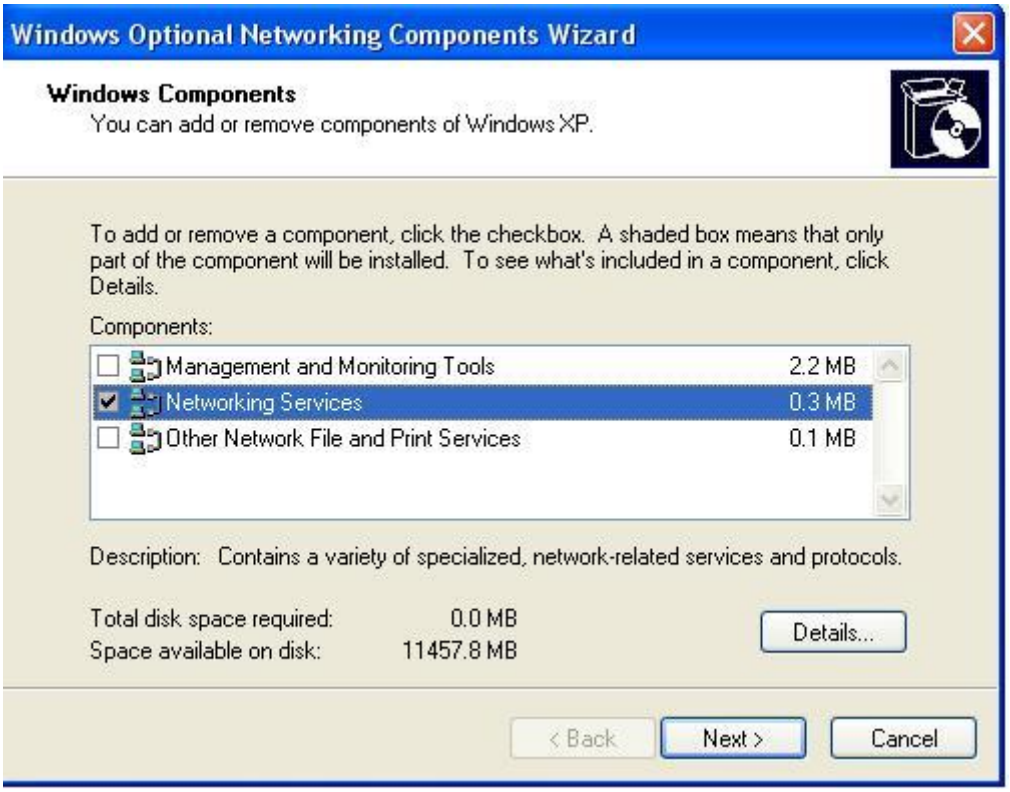
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….



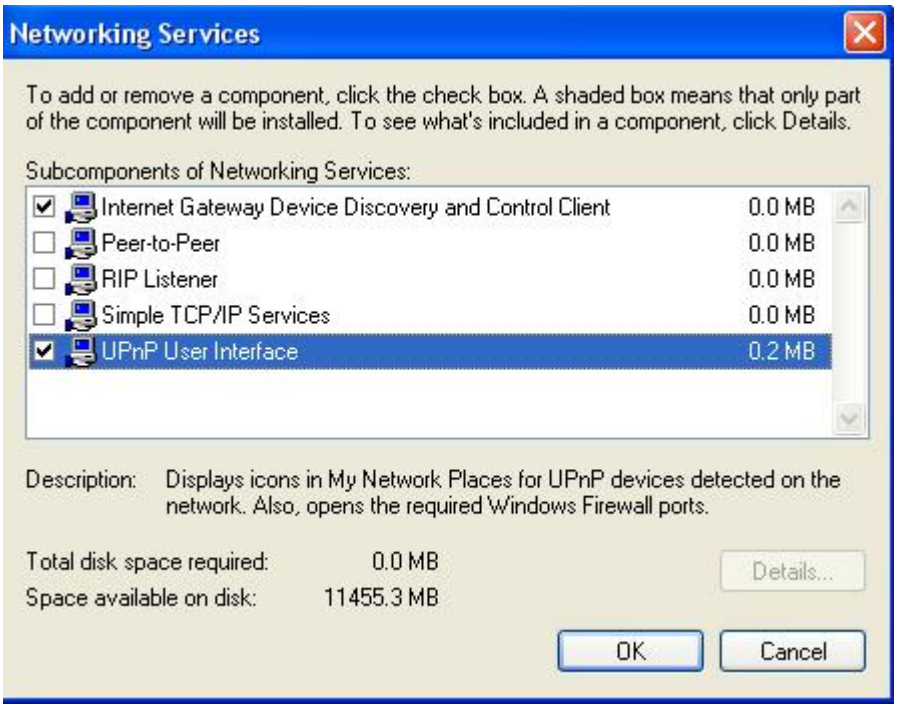
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 2.2 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.1 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 11457.8 MB
Details...
< Back
Next >
Cancel

Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 0.0 MB
Space available on disk: 11455.3 MB
Details...
OK
Cancel

Auto-discover Your UPnP-enabled Network Device

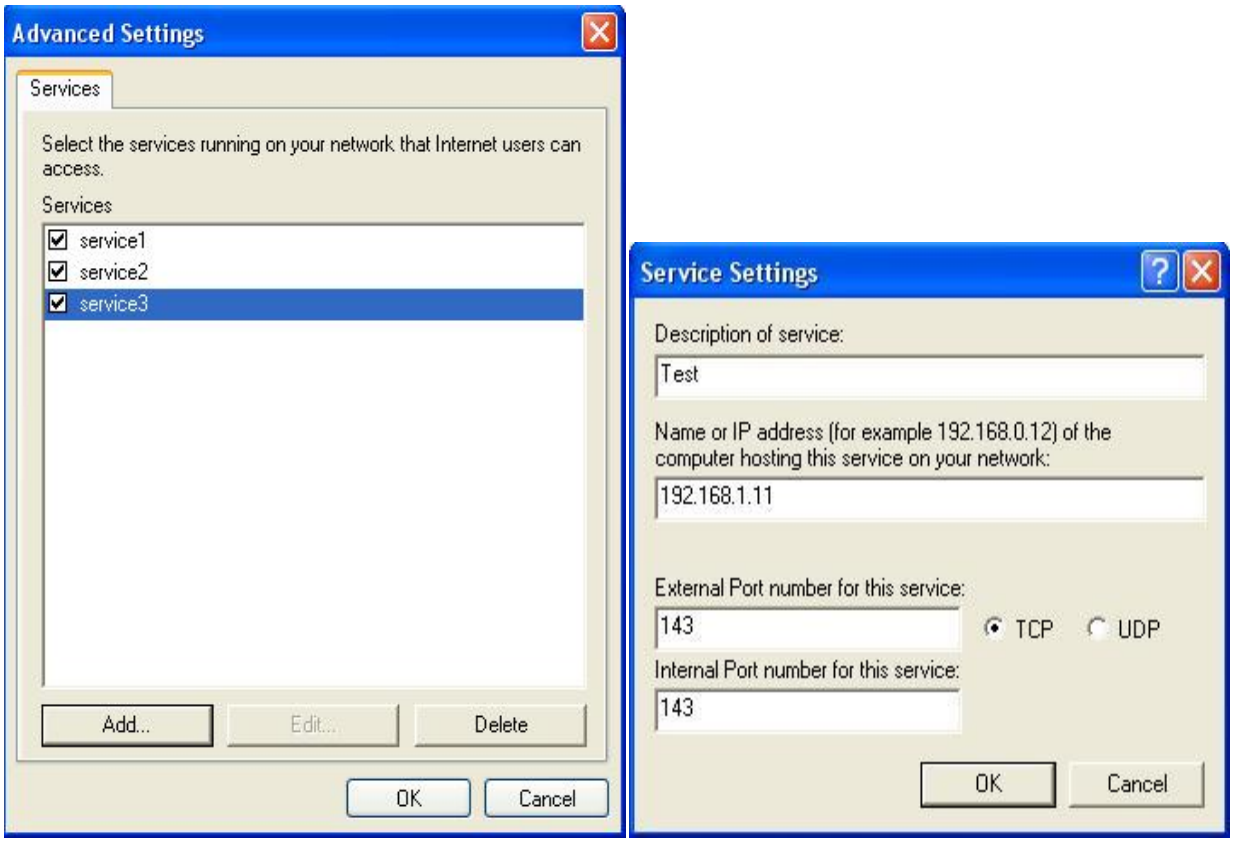
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.

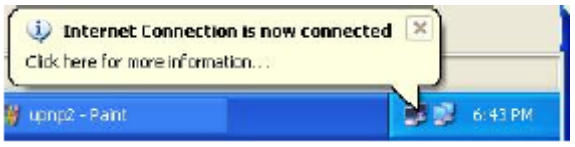
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

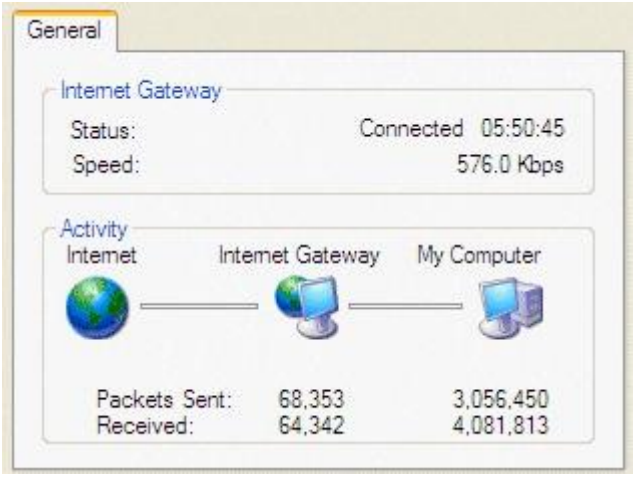
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Easy Management and Access to the Router

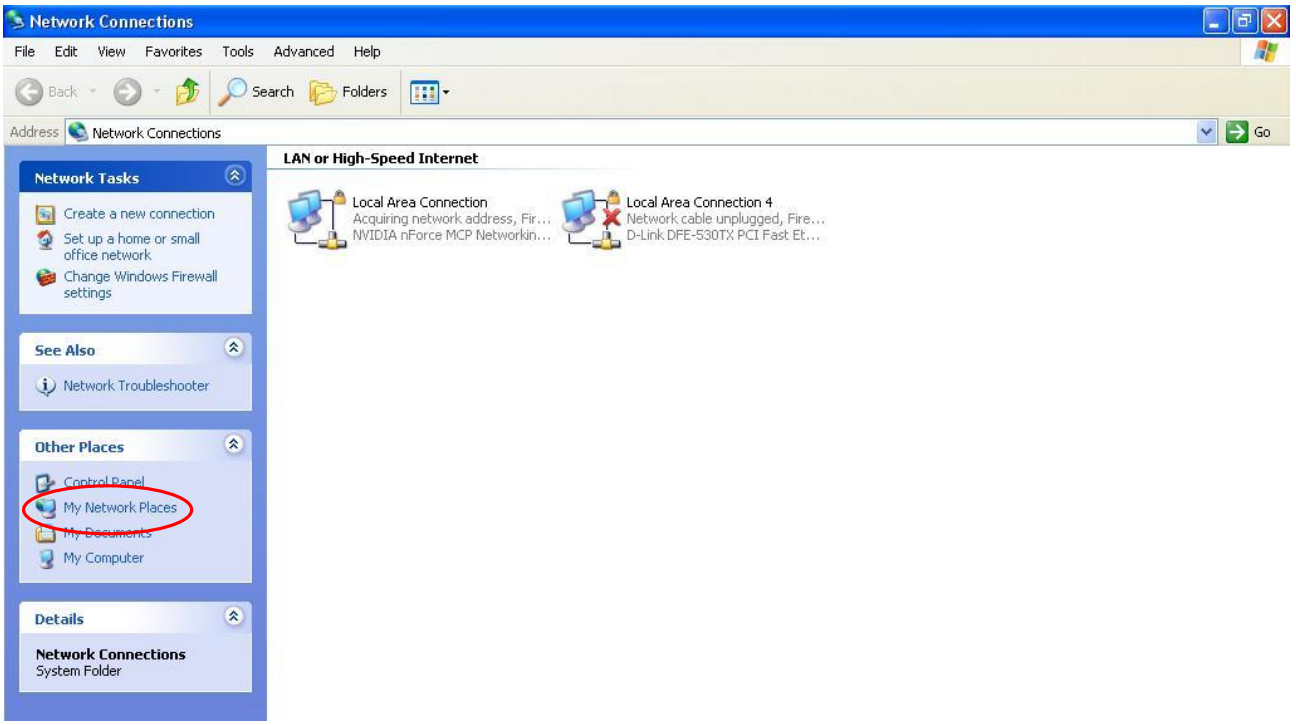
With UPnP, you can access web-based configuration for the **BEC 6800RUL (4G_LTE OUTDOOR ROUTER)** without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your **BEC 6800RUL (4G_LTE OUTDOOR ROUTER)** and select Invoke. The web configuration login screen displays.

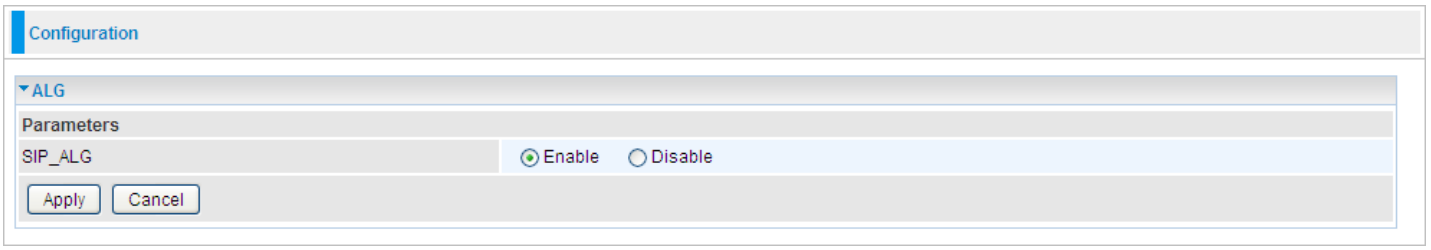
Step 6: Right-click on the icon of your **BEC 6800RUL (4G_LTE OUTDOOR ROUTER)** and select Properties. A properties window displays basic information about the router.

SIP_ALG

Select **Enable** to activate **SIP ALG** feature or Disabled to disable this feature.

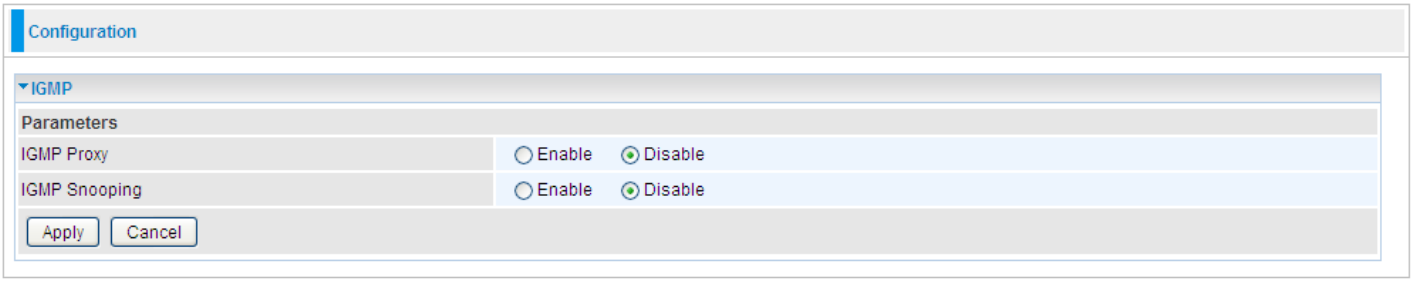
The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such voice and video calls over Internet protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. It is a text-based Application Layer protocol.

But as many use NAT to communicate with the public networks, and the IP address and port combination in SIP packets are needed for addressing, we must come up with an effective way to deal with SIP NAT traversal. SIP ALG is an easy solution with which you are only required to enable SIP ALG on NAT application in this router to easily experience the smooth SIP connection between private networks and public networks or even in two private networks with your VoIP devices.



IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

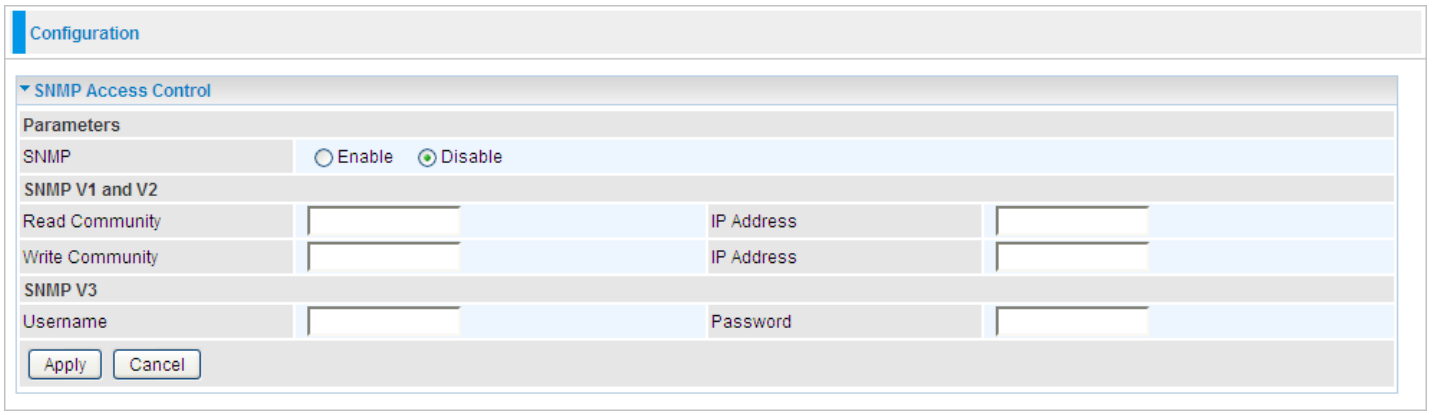


IGMP Proxy: Accepting multicast packet. Default is set to **Disable.**

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function - Simple Network Management Protocol.



SNMP V1 and V2

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

☑ System group
☑ Interfaces group
☑ Address Translation group
☑ IP group
☑ ICMP group
☑ TCP group
☑ UDP group
☒ EGP (not applicable)
☑ Transmission
☑ SNMP group

From RFC1650 (EtherLike-MIB):

☑ dot3Stats

From RFC 1493 (Bridge MIB):

☑ dot1dBase group
☑ dot1dTp group
☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

☑ pppLink group
☒ pppLqr group

From RFC 1472 (PPP/Security MIB):

☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

☑ PPP Bridge Group

From RFC1573 (IfMIB):

☑ ifMIBObjects Group

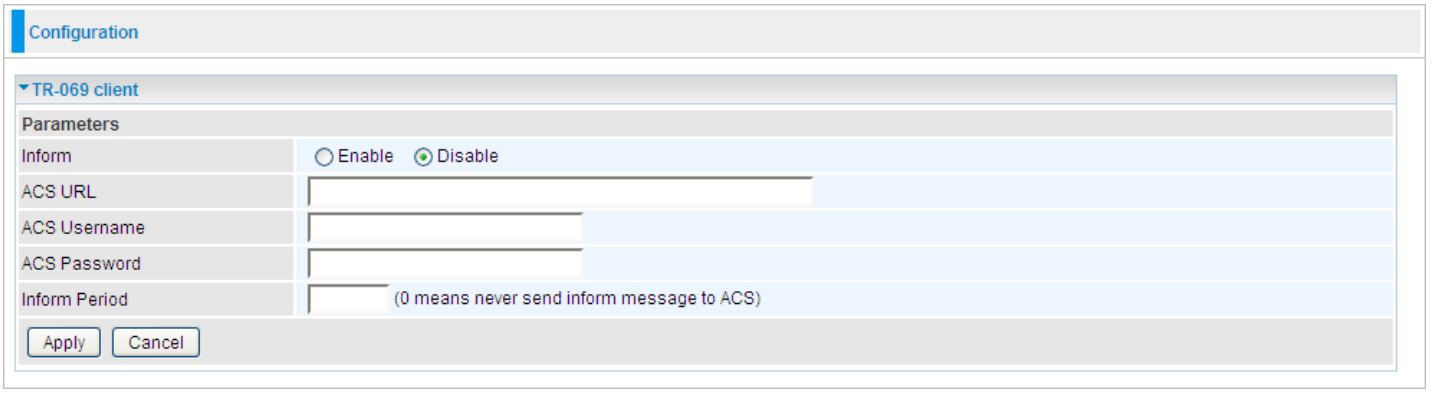
From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

TR-069 Client

TR069, (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Inform: Enable to authorize CPE to send Inform message to automatically connect to ACS.

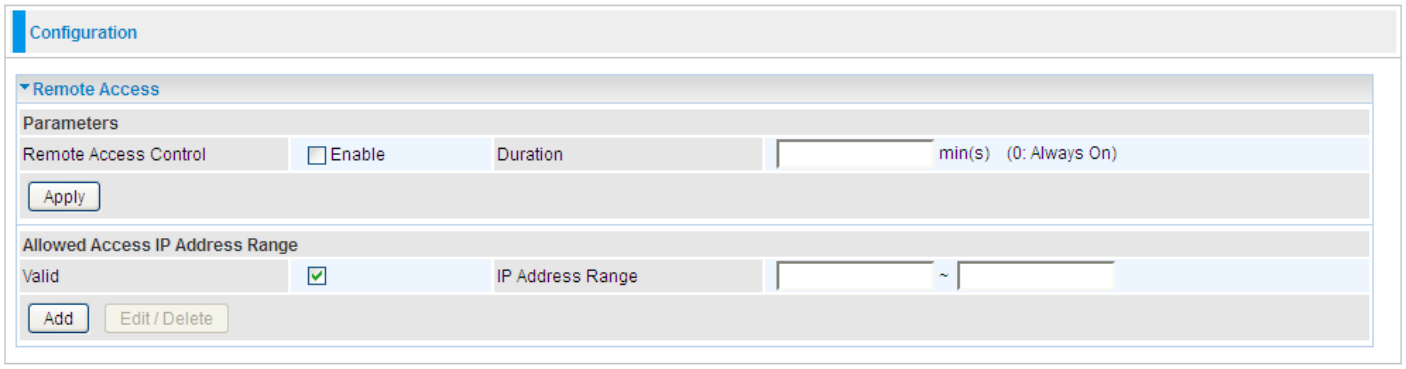
ACS URL: Enter the ACS server accessing URL.

ACS Username: Set the ACS user name for ACS authentication to the connection from CPE.

ACS Password: Set the ACS server login password.

Inform Period: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS.

Remote Access



Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

Allowed Access IP Address Range

Valid: Select Valid to allow remote management from these IP ranges.

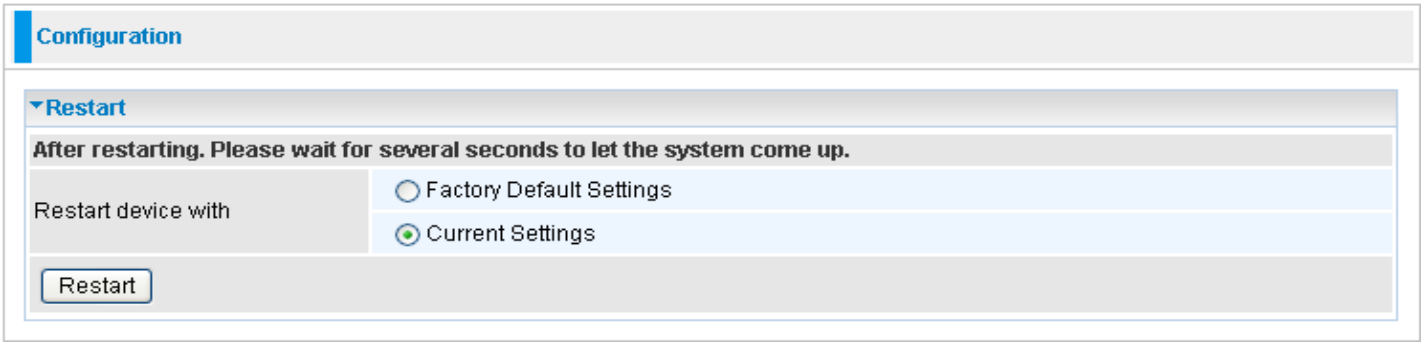
IP Address Range: Specify what IP address to be allowed to access device from remote side. Clink Add to insert management IP address list.

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "**Save Config**" and click "**Apply**" to write your new configuration to FLASH.

Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes.

You can modify this value using the **Advanced / Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

CHAPTER 6: TROUBLESHOOTING

If your Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Recovery Procedures

Problem	Suggested Action
- The front LEDs display incorrectly **- Still cannot access to the router management interface after pressing the RESET button.** **- Software / Firmware upgrade failure**	1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately. 2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems please contact the dealer from where you purchased your product.

Contact BEC @ http://www.bectechnologies.net

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows ME, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

V1.06.r18t.dc30